LANDesk®

Management Suite 9.5

Benutzerhandbuch

LANDesk® SOFTWARE

Copyright © 2002-2012, LANDesk Software, Inc. und angeschlossene Unternehmen. Alle Rechte vorbehalten. LANDesk und die zugehörigen Logos sind entweder eingetragene Marken oder Marken von LANDesk Software, Inc. oder angeschlossenen Unternehmen in den Vereinigten Staaten von Amerika und/oder in anderen Ländern. Andere Marken und Namen können Eigentum ihrer jeweiligen Inhaber sein.

LANDesk übernimmt keine Verantwortung für Fehler in diesem Dokument und behält sich das Recht vor, dieses Dokument und damit im Zusammenhang stehende Produktspezifikationen und Beschreibungen jederzeit und ohne vorherige Ankündigung zu ändern. LANDesk lehnt jegliche Verpflichtung zur Aktualisierung der in diesem Dokument enthaltenen Informationen ab. Dieses Dokument wird "WIE BESEHEN" bereitgestellt und beinhaltet keinerlei ausdrückliche oder stillschweigende Haftung, Garantie oder Lizenz, einschließlich aber nicht beschränkt auf die Eignung für einen bestimmten Zweck, Marktgängigkeit, Nichtverletzung von geistigen Eigentumsrechten oder anderen Rechten Dritter. Kein LANDesk Produkt, auf das in diesem Dokument verwiesen wird, eignet sich für den Einsatz in medizinischen, lebensrettenden oder lebenserhaltenden Systemen. Möglicherweise können Dritte intellektuelle Eigentumsrechte in Bezug auf dieses Dokument und die darin behandelten Technologien geltend machen.

Zuletzt überarbeitet am: 12/20/2012

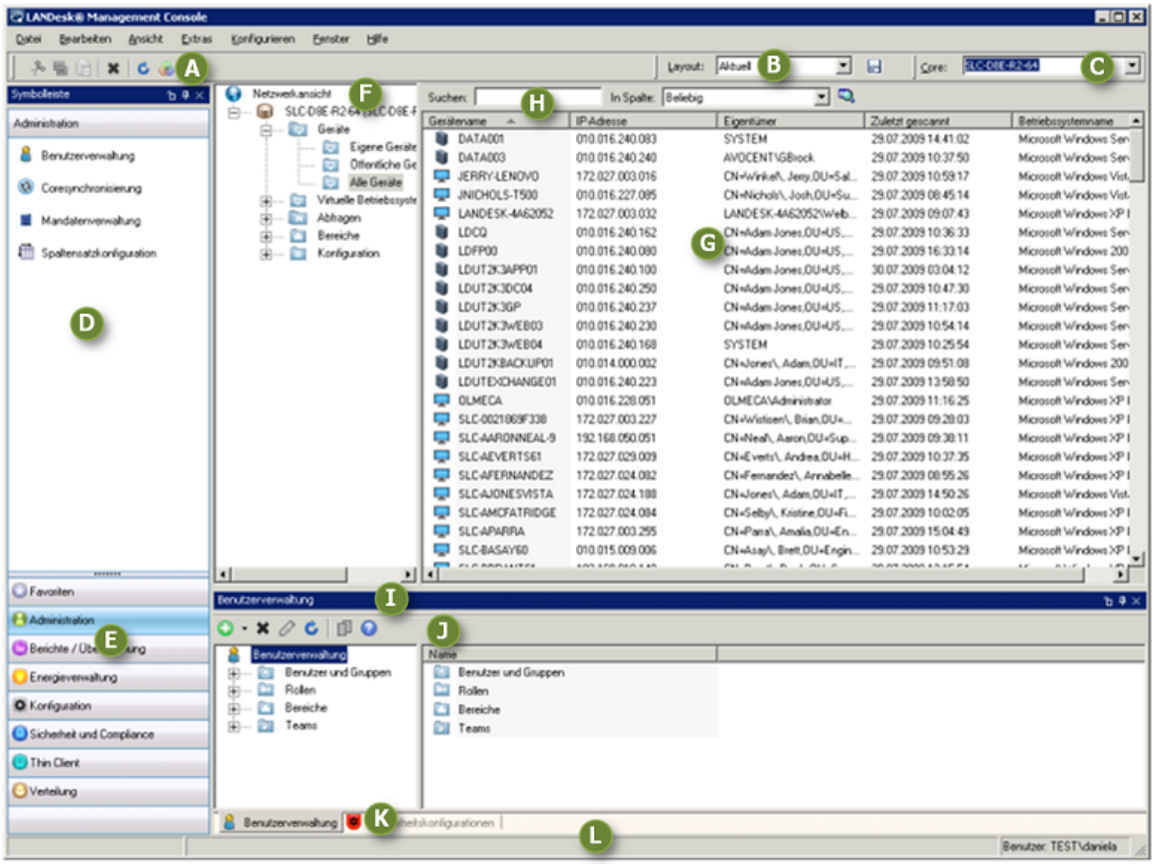
Inhalt

Inhalt ... 3
Konsole ... 4
Benutzerverwaltung ... 40
Corekonfiguration ... 63
Konfigurieren von Corediensten ... 84
Coresynchronisierung ... 97
Agentenkonfiguration ... 105
Agentenüberwachung ... 148
Inventar ... 156
Abfragen/Verzeichnis-Manager ... 193
Auditing ... 201
Berichte ... 209
Planen von Tasks ... 242
Local Scheduler ... 250
Remotesteuerung ... 257
Softwareverteilung/Verteilungspakete/Verteilungsmethoden ... 269
Verwaltung von Anwendungsrichtlinien (Application Policy Management) ... 318
Softwarelizenzüberwachung ... 323
Erkennung nicht verwalteter Geräte ... 362
Betriebssystembereitstellung ... 378
Versorgung (Provisioning) ... 444
LANDesk SmartVue ... 488
Lokale Konten ... 499
Verwalten von Macintosh-Geräten ... 505
Einführung in LANDesk Security Suite ... 526
Netzwerkzugriffskontrolle (Network Access Control) ... 537
Patch und Compliance ... 578
Sicherheitskonfigurationen ... 692
Sicherheitsaktivität ... 706
Endpunktsicherheit ... 713
LANDesk Antivirus ... 751
Credant Data Protection ... 802
LaunchPad Link-Manager ... 812
Energieverwaltung ... 815
Alarmfunktion ... 832
Intel vPro ... 877
Rollup-Cores ... 904
Bevorzugte Server und Inhaltsreplikation ... 912
Mandantenverwaltung ... 926
Anwendungsvirtualisierung ... 931
Webkonsole ... 934
Inventory Manager ... 985
HP Hardware Management ... 986

Konsole

Übersicht über die Konsole

Die Administratorkonsole ist der zentrale Ausgangspunkt für den Zugriff auf alle Netzwerkverwaltungsfunktionen. Von dieser zentralen Konsole aus können Sie Software- oder Konfigurationseinstellungen verteilen und aktualisieren, Hard- und Softwareprobleme diagnostizieren, Betriebssystemabbilder bereitstellen, Benutzerprofile migrieren und mithilfe der rollenbasierten Administration festlegen, wie Benutzer auf Funktionen und Geräte zugreifen. Darüber hinaus können Sie Remotesteuerungsfunktionen einsetzen, um Endanwender zu schulen oder um Probleme zu lösen und für vieles andere.



***A** Symbolleiste der Konsole **B** Layout-Menü, **C** Coreserver-Menü, **D** Extras, **E** Extra-Gruppen, **F** Netzwerkansicht, **G** Ergebnisliste, **H** Suchleiste, **I** Extra-Bereich, **J** Extras-Symbolleiste, **K** Extra-Registerkarten, **L** Statusleiste*

In den Hilfethemen in diesem Abschnitt erfahren Sie, wie Sie die Konsole steuern und verwenden, um Geräte anzuzeigen und zu organisieren und auf die verschiedenen Verwaltungsextras zuzugreifen.

Umfassende und aktuelle Informationen zur Installation und Konfiguration

Je nachdem, wie umfassend der Verwaltungsbedarf Ihres Netzwerks ist, kann Ihre Lösung mehrere Coreserver und Datenbanken umfassen. Informationen zur Installation eines LANDesk Management Suite Coreservers und einer Konsole, zu zusätzlichen Konsolen, zur Webkonsole und zur Verwaltung mehrerer Coreserver und Datenbanken finden Sie in der auf der LANDesk Benutzercommunity-Website bereitgestellten Dokumentation.

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter LANDesk Benutzercommunity – Startseite

Verwandte Themen

Konsolensetup-Assistenten

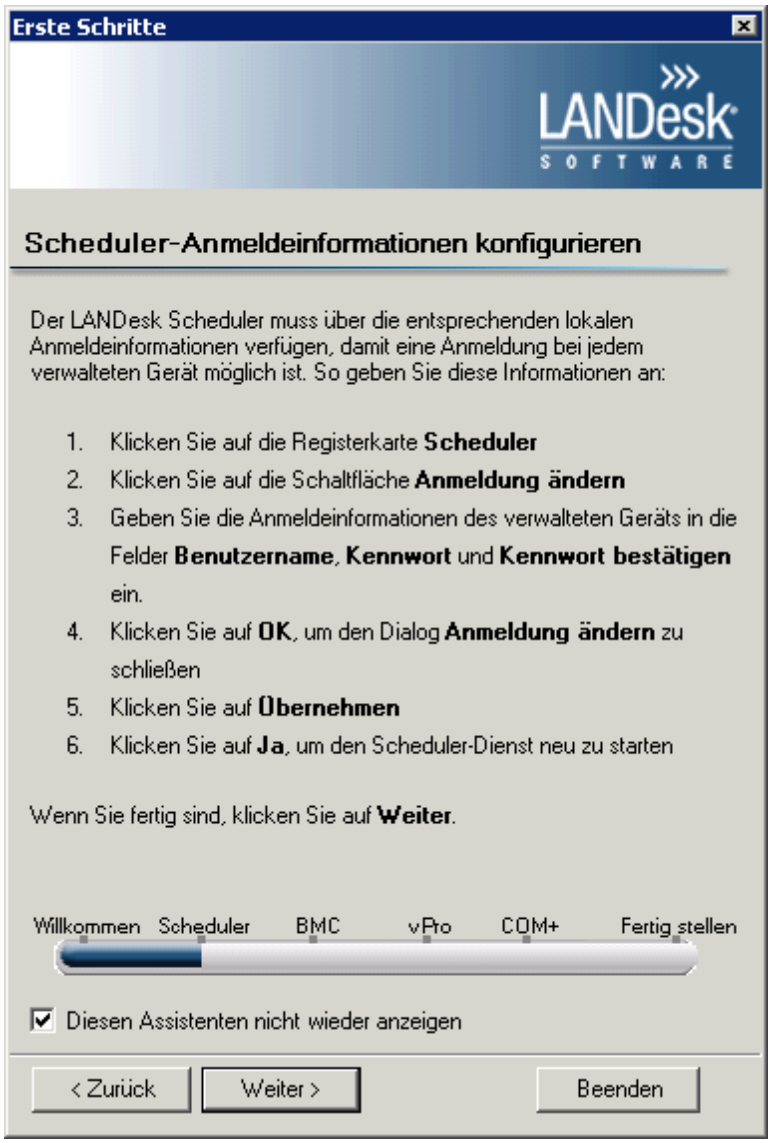
Für mehrere Bereiche von LANDesk Management Suite stehen Assistenten zur Verfügung. Diese Assistenten durchlaufen eine Reihe von Anweisungen, während der Benutzer die beschriebenen Schritte ausführt.

Bei einer Neuinstallation werden die Assistenten automatisch anzeigt und können später jederzeit über das Menü **Hilfe** aufgerufen werden. Sie können den Schritte im Assistenten folgen, um mehr über die spezifische Funktion oder Funktionalität zu erfahren. Sie können aber auch das Kontrollkästchen **Diesen Assistenten nicht wieder anzeigen** markieren, damit der Assistent nicht erneut automatisch angezeigt wird.

Der Assistent "Erste Schritte"

Der Assistent **Erste Schritte** unterstützt Sie bei der Konfiguration von LANDesk Management Suite für die folgende Funktionen:

- Tasks auf Ihren verwalteten Geräten planen
- Intel vPro- und IPMI-Geräte verwalten
- Verwaltete Geräte remote steuern
- Domänenbenutzer in der Webkonsole anzeigen


Erste Schritte
LANDesk
SOFTWARE
Scheduler-Anmeldeinformationen konfigurieren
Der LANDesk Scheduler muss über die entsprechenden lokalen Anmeldeinformationen verfügen, damit eine Anmeldung bei jedem verwalteten Gerät möglich ist. So geben Sie diese Informationen an:
1. Klicken Sie auf die Registerkarte Scheduler
2. Klicken Sie auf die Schaltfläche Anmeldung ändern
3. Geben Sie die Anmeldeinformationen des verwalteten Geräts in die Felder Benutzername, Kennwort und Kennwort bestätigen ein.
4. Klicken Sie auf OK, um den Dialog Anmeldung ändern zu schließen
5. Klicken Sie auf Übernehmen
6. Klicken Sie auf Ja, um den Scheduler-Dienst neu zu starten
Wenn Sie fertig sind, klicken Sie auf Weiter.
Willkommen
Scheduler
BMC
vPro
COM+
Fertig stellen
Diesen Assistenten nicht wieder anzeigen
< Zurück
Weiter >
Beenden

Der Assistent "Agenten erkennen und installieren"

Der Assistent **Agenten erkennen und installieren** unterstützt den Benutzer bei der Konfiguration von LANDesk Management Suite für die folgende Funktionen:

- Erkennung: Sucht nach Geräten im Netzwerk, die LANDesk Management Suite nicht bekannt sind. Für das Scannen des Netzwerks können IP-Adressbereiche angegeben werden.
- Agenten bereitstellen: Installiert den LANDesk Management-Agenten auf Geräten, die verwaltet werden sollen.

Der Assistent "Sicherheits-Updates"

Der Assistent **Sicherheits-Updates** unterstützt den Benutzer beim Download und bei der Verwaltung von Sicherheits- und Patchdateien sowie Anfälligkeitsdefinitionsdateien von LANDesk Inhaltsservern. Dieser Assistent hilft bei der Konfiguration von Tasks für den Download von Updates, dem Starten der Tasks und der Planung zukünftiger Downloads.

Der Assistent "Rollen und Gruppen erstellen"

Der Assistent **Benutzerverwaltung** unterstützt Sie bei der Durchführung der Schritte, die zur Verwaltung des Zugriffs auf Geräte im Netzwerk notwendig sind und um zu definieren, welche Extras oder spezifischen Funktionen auf diesen Geräten eingesetzt werden können. Er führt Sie durch den Prozess der Erstellung eines Bereichs, einer Rolle und einer Gruppenberechtigung für Benutzer.

Starten der Konsole

So starten Sie die Konsole

1. Klicken Sie auf **Start** > **Programme** > **LANDesk > Management Suite**. (Der eigentliche Programmname lautet möglicherweise anders, je nachdem, welches LANDesk Produkt installiert ist und mit welcher Lizenz Ihr Coreserver aktiviert wurde.)
2. Geben Sie den Benutzernamen und das Kennwort ein.

   Halten Sie beim Herstellen einer Verbindung zu einem Remote-Coreserver die üblichen Windows-Richtlinien für die Remote-Anmeldung ein (d.h., wenn der Benutzer ein lokaler Benutzer dieses Coreservers ist, geben Sie lediglich den Benutzernamen ein; wenn es sich hingegen um einen Domänenbenutzer handelt, geben Sie den Domänennamen\Benutzernamen ein).
3. Wählen Sie den Coreserver aus, mit dem Sie eine Verbindung herstellen möchten. Der Benutzer muss über die erforderlichen Anmeldeinformationen für die Authentifizierung bei diesem Coreserver verfügen.
4. Klicken Sie auf **OK**.

Die Konsole wird mit dem Layout geöffnet (Format, Position, geöffnete Extra-Fenster usw.), das vor dem Abmelden dieses Benutzers verwendet wurde.

Für Zusatzkonsolen müssen die Anmeldeinformationen, mit denen Sie sich bei Management Suite anmelden, mit den Anmeldeinformationen übereinstimmen, die für die Laufwerke verwendet werden, die Sie dem Coreserver zugeordnet haben. Andernfalls wird möglicherweise ein Fehler "Mehrere Verbindungen" im Anmeldedialogfeld der Konsole angezeigt.

Informationen zum Dialogfeld für die Anmeldung

Verwenden Sie dieses Dialogfeld, um die Konsole zu starten und eine Verbindung mit einem Coreserver herzustellen.

- **Benutzername:** Identifiziert einen LANDesk Benutzer. Es kann sich dabei um einen Administrator-Benutzer oder um einen anderen Benutzertyp mit eingeschränktem Zugriff handeln (siehe "Benutzerverwaltung" auf Seite 40). Der Benutzer muss ein Mitglied einer LANDesk Gruppe auf dem Coreserver sein. Halten Sie die üblichen Windows-Richtlinien für die Remoteanmeldung ein (d. h., wenn der Benutzer ein lokaler Benutzer dieses Coreservers ist, geben Sie lediglich den Benutzernamen ein; wenn es sich hingegen um einen Domänenbenutzer handelt, geben Sie den

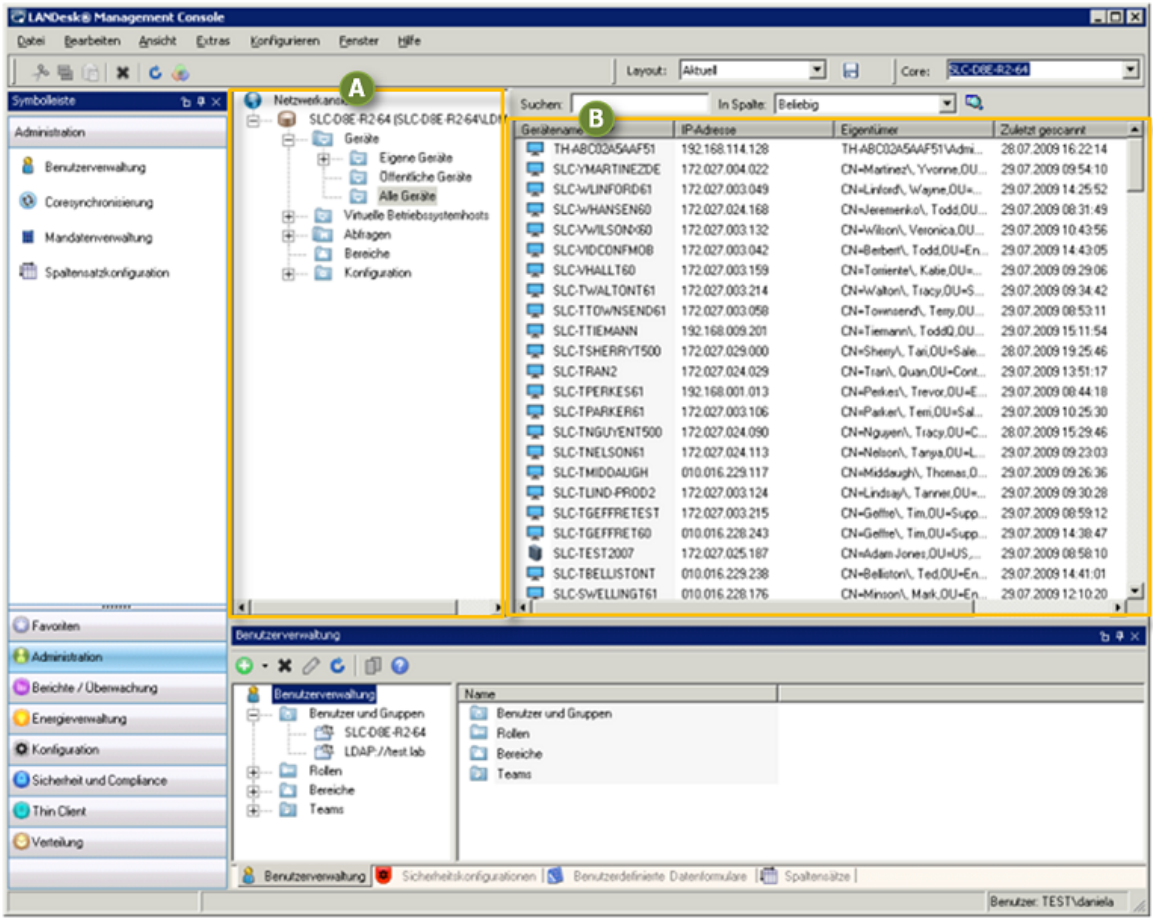
Domänennamen\Benutzernamen ein).

- **Kennwort:** Das Kennwort des Benutzers. (**HINWEIS:** Wenn ein LANDesk Administrator das Kennwort eines anderen Benutzers, beispielsweise eines zusätzlichen Konsolenbenutzers, ändert, wird das neue Kennwort erst wirksam, nachdem dieser Benutzer seine Konsole neu gestartet hat. Der Benutzer gibt dann das neue Kennwort ein, um sich bei der Konsole anzumelden.)
- **Coreserver:** Der Coreserver, mit dem Sie eine Verbindung herstellen möchten. Diese Liste entspricht der Coreserver-Liste, die in der Symbolleiste der Konsole zur Verfügung steht.

Grundlegendes zur Netzwerkansicht

Die Netzwerkansicht ist das Hauptfenster der Konsole und Ausgangspunkt für die meisten Verwaltungstasks. In der Netzwerkansicht können Sie die Inventardaten des Geräts anzeigen, Abfragen für die Suche und die Gruppierung von Geräten erstellen, Geräte für die Remotesteuerung auswählen usw.

Die aus zwei Bereichen bestehende Netzwerkansicht bleibt während der gesamten Sitzung geöffnet. Der linke Fensterbereich **(A)** zeigt eine hierarchische Strukturansicht des Coreservers bzw. der Datenbank, mit dem/der Sie zurzeit verbunden sind. Darüber hinaus sehen Sie in diesem Fensterbereich die mit dem Coreserver bzw. mit der Datenbank verbundenen **Geräte-**, **Abfrage-** und **Konfigurationsgruppen**. Sie können die Objekte in der Strukturansicht nach Bedarf erweitern oder reduzieren. Im rechten Bereich **(B)** der Netzwerkansicht wird eine detaillierte Liste der Elemente der ausgewählten Gruppe angezeigt.



***A** Bereich "Netzwerkansicht", **B** Listenansicht "Ausgewählte Elemente"*

Sie können die Netzwerkansicht und die zugehörigen Fensterbereiche und Spalten vergrößern und verkleinern; Sie können sie jedoch nicht schließen. Die Netzwerkansicht ist im Gegensatz zu den Extra-Fenstern nicht verankerbar.

HINWEIS: Rollenbasierte Administration
Welche Geräte Sie in der Netzwerkansicht anzeigen und verwalten und welche Verwaltungstools Sie verwenden können, hängt von den Zugriffsrechten und Gerätebereichen ab, die Ihnen vom Administrator zugewiesen wurden. Weitere Informationen finden Sie unter "Benutzerverwaltung" auf Seite 40.

Die **Netzwerkansicht** enthält folgende Gruppen und Untergruppen:

Core

Das **Core**-Objekt identifiziert den Coreserver, mit dem Sie gegenwärtig verbunden sind. Das **Core**-Objekt befindet sich direkt unter dem Stamm der Netzwerkansicht und kann erweitert und reduziert werden.

Syntax des Core-Objektnamens

Die Syntax für den Namen des Core-Objekts lautet:

Servername\Datenbankinstanz

Geräte

Die Gruppe **Geräte** enthält die folgenden Geräteuntergruppen:

- **Eigene Geräte:** Führt auf der Basis des Benutzerbereichs die Geräte für den aktuell angemeldeten Benutzer auf. Benutzer können nur unter **Eigene Geräte** Untergruppen für Geräte erstellen. Sie können Geräte zur Gruppe **Eigene Geräte** oder zu einer Untergruppe hinzufügen, indem Sie die Geräte aus den Gruppen **Öffentliche Geräte** und **Alle Geräte** kopieren. Außerdem können Benutzer unter **Öffentliche Geräte** und **Alle Geräte** auf Geräte klicken und sie in die Gruppe **Eigene Geräte** ziehen.

HINWEIS: Ziehen und Ablegen von Elementen in der Netzwerkansicht
Wenn Sie auf ein Element klicken, um es in eine andere Gruppe in der Netzwerkansicht zu ziehen, zeigt der Cursor an, wo ein Ablegen möglich bzw. nicht möglich ist. Wenn beim Ziehen des Cursors über ein Gruppenobjekt ein Pluszeichen (+) angezeigt wird, so bedeutet dies, dass Sie das Element zu dieser Gruppe hinzufügen können; das Verbotszeichen (der durchgestrichene Kreis) bedeutet, dass Sie das Element nicht zu dieser Gruppe hinzufügen können.

- **Öffentliche Geräte:** Listet Geräte auf, die von einem Administrator (d. h. einem Benutzer, der das LANDesk Administrator-Recht besitzt) aus der Gruppe **Alle Geräte** hinzugefügt wurden. Ein Administrator kann alle Geräte in dieser Gruppe anzeigen, während andere Benutzer nur die Geräte anzeigen können, die zu ihrem Bereich gehören. Außerdem kann ein Administrator eine Untergruppe unter **Öffentliche Geräte** erstellen.
- **Alle Geräte:** Erstellt eine einfache Liste (keine Untergruppen) mit allen Geräten, die für den zurzeit angemeldeten Benutzer (abhängig von dessen Bereich) sichtbar sind. Für einen Administrator führt **Alle Geräte** alle verwalteten Geräte auf, die in die Coredatenbank gescannt wurden. Mit dem Standard LANDesk Agenten konfigurierte Geräte werden automatisch in der Gruppe **Alle Geräte** angezeigt, wenn sie mit dem Inventarscanner in die Coredatenbank gescannt werden.

Bei regulären Benutzern setzt sich die Gruppe "Alle Geräte" aus den Gruppen **Eigene Geräte** und **Öffentliche Geräte** ihrer Benutzer zusammen.

Administratoren und Benutzer können Inventarberichte für die Geräte in dieser Gruppe ausführen.

Sie können auch manuell Computer zur Netzwerkansicht hinzufügen, indem Sie mit der rechten Maustaste auf die Gruppe **Alle Geräte** klicken, auf **Neuen Computer einfügen** klicken, die Geräte- und Netzwerkinformationen eingeben und auf **OK** klicken. Diese Computer werden auch in der Untergruppe "Vom Benutzer hinzugefügte Computer" unter der Gruppe "Konfiguration" angezeigt.

Virtuelle Betriebssystemhosts

Die Gruppe "Virtuelle Betriebssystemhosts" zeigt die virtuellen VMware ESX Host-Server an. Die Gruppe "Virtuelle Betriebssystemhosts" enthält folgende Konfigurationsgruppen:

- **Eigene virtuelle Betriebssystem-Hosts:** Führt die virtuellen Betriebssystem-Hosts für den derzeit angemeldeten Benutzer auf, basierend auf dem Benutzerbereich. Ein Benutzer kann Geräteuntergruppen nur unter "Eigene virtuelle Betriebssystem-Hosts" erstellen.
  Benutzer können Geräte zu ihrer Gruppe "Eigene virtuelle Betriebssystem-Hosts" oder zu einer zugehörigen Untergruppe hinzufügen, indem Sie die Geräte aus den Gruppen "Öffentliche virtuelle Betriebssystem-Hosts" und "Alle virtuellen Betriebssystem-Hosts" kopieren. Benutzer können virtuelle Betriebssystem-Hosts aus den Gruppen "Öffentliche virtuelle Betriebssystem-Hosts" und "Alle virtuellen Betriebssystem-Hosts" auch anklicken und in ihre Gruppe "Eigene virtuelle Betriebssystem-Hosts" ziehen.
- **Öffentliche virtuelle Betriebssystem-Hosts:** Listet Geräte, die ein Management Suite Administrator aus der Gruppe "Alle virtuellen Betriebssystem-Hosts" hinzugefügt hat. Benutzer mit den Rechten eines LANDesk Administrators sehen alle Geräte in dieser Gruppe, während andere Konsolenbenutzer nur die Geräte sehen können, die für ihren Bereich zugelassen sind. Nur ein Administrator kann eine Untergruppe unter "Öffentliche virtuelle Betriebssystem-Hosts" erstellen.
- **Alle virtuellen Betriebssystem-Hosts:** Erstellt eine eindimensionale Liste (keine Untergruppen) mit allen virtuellen Betriebssystem-Hosts, die für den zurzeit angemeldeten Benutzer, abhängig von dessen Bereich, sichtbar sind. Für einen Administrator führt "Alle virtuellen Betriebssystem-Hosts" alle verwalteten virtuellen Betriebssystem-Hosts auf, die in die Datenbank gescannt wurden. Mit dem LANDesk Standardagenten konfigurierte virtuelle Betriebssystemhosts werden automatisch in der Gruppe/dem Ordner "Alle virtuellen Betriebssystem-Hosts" angezeigt, wenn sie mit dem Inventarscanner in die Datenbank gescannt werden.
- **Benutzer – virtuelle Betriebssystemhosts:** Listet alle in der Datenbank enthaltenen virtuellen Betriebssystem-Hosts nach Benutzeruntergruppen organisiert auf. Benutzeruntergruppen werden mit den Anmeldekennungen der Benutzer benannt (d. h. Computername\Benutzerkonto oder Domäne\Benutzerkonto). Jede Benutzergruppe enthält die virtuellen Betriebssystem-Hosts, die in der Gruppe "Eigene virtuelle Betriebssystemhosts" des jeweiligen Benutzers angezeigt werden.

Abfragen

Die Gruppe **Abfragen** enthält die folgenden Abfrageuntergruppen:

- **Eigene Abfragen:** Führt Abfragen auf, die entweder vom gegenwärtig angemeldeten Benutzer erstellt oder von einem Administrator in die Gruppe **Benutzerabfragen** eines Benutzers eingefügt wurden. Ein Benutzer kann Abfragegruppen und Abfragen unter der Gruppe **Eigene Abfragen** erstellen, ändern und löschen. Er kann auch Abfragen in diese Gruppe aus der Gruppe **Öffentliche Abfragen** kopieren.

Jede Abfrage, die ein Benutzer ausführt, ist auf den Gerätebereich begrenzt, der durch den Benutzerbereich definiert ist. Wenn einem Benutzer beispielsweise der Bereich **Alle Rechner** zugeordnet wurde, durchsucht die Abfrage alle Geräte in der Coredatenbank; wenn der Benutzerbereich jedoch auf 20 Rechner begrenzt ist, werden nur 20 Rechner von der Abfrage durchsucht. Weitere Informationen zum Erstellen von Abfragen finden Sie unter "Abfragen/Verzeichnis-Manager" auf Seite 193.

- **Öffentliche Abfragen:** Führt Abfragen auf, die ein Administrator oder ein Benutzer mit PQM (Public Query Management)-Recht hinzugefügt hat. Nur Benutzer, die entweder über LANDesk Administrator- oder PQM-Rechte verfügen, können Abfragegruppen oder Abfragen in der Gruppe **Öffentliche Abfragen** hinzufügen, ändern oder löschen. Die in dieser Gruppe enthaltenen Abfragen sind jedoch für alle Benutzer sichtbar und können von jedem Benutzer in die Gruppe **Eigene Abfragen** kopiert werden.
- **Alle Abfragen:** Erstellt eine einfache Liste (keine Untergruppen) mit allen Geräten, die für den zurzeit angemeldeten Benutzer (abhängig von dessen Bereich) sichtbar sind. Die Gruppe **Alle Abfragen** setzt sich aus den Gruppen **Eigene Abfragen** und **Öffentliche Abfragen** des Benutzers zusammen.

Administratoren können diese Gruppe verwenden, um die Abfragen eines Benutzers für den Bereich dieses Benutzers auszuführen (als wären sie dieser Benutzer). Somit kann ein Administrator eine genaue Vorschau der Ergebnisse anzeigen, die auch ein Benutzer sieht, wenn er eine Abfrage ausführt.

Bereiche

Die Netzwerkansicht umfasst einen Shortcut für die Anzeige vorhandener Bereiche bzw. zur Bearbeitung und Erstellung neuer Bereiche. Ferner können Sie die Felder definieren, die Sie in der Netzwerkansicht anzeigen möchten. Einzelheiten zur Erstellung und Verwendung von Bereichen finden Sie unter "Erstellen eines Bereichs" auf Seite 58.

Konfiguration

Die Gruppe **Konfiguration** enthält folgende Konfigurationsuntergruppen.

- **PXE-Warteschlange:** Führt PXE-Warteschlangen und Geräte auf, die sich in der PXE-Warteschlange befinden.
- **Bare Metal Server:** Führt Bare-Metal-Geräte auf, die für Versorgungstasks erstellt wurden.
- **PXE-Versorgung (Windows PE):** Führt Geräte auf, die das Ziel von Microsoft Windows PE-Versorgungstasks sind.
- **Multicast-Domänenrepräsentanten:** Führt konfigurierte Multicast-Domänenrepräsentanten auf, die für die Softwareverteilung mit Load Balancing verwendet werden können. Weitere Informationen finden Sie unter "Softwareverteilung mit Targeted Multicast" auf Seite 284.
- **PXE-Repräsentanten:** Führt als PXE-Repräsentanten konfigurierte Geräte auf, die Betriebssystemabbilder auf Geräten in ihrem Subnetz bereitstellen können.
- **Ausstehende nicht verwaltete Clientbereitstellungen:** Listet Geräte auf, die mit dem Extra "Erkennung nicht verwalteter Geräte" gefunden wurden und auf einen Agenten-Konfigurationstask warten. Weitere Informationen finden Sie unter "Erkennung nicht verwalteter Geräte – Übersicht" auf Seite 362.
- **Vom Benutzer hinzugefügte Computer:** (Nur Administrator) Führt Computer auf, die über das Dialogfeld "Neuen Computer einfügen" (mit der rechten Maustaste auf die Gruppe **Alle Geräte** klicken) manuell zur Netzwerkansicht hinzugefügt wurden.

Inspector-Ergebnisse

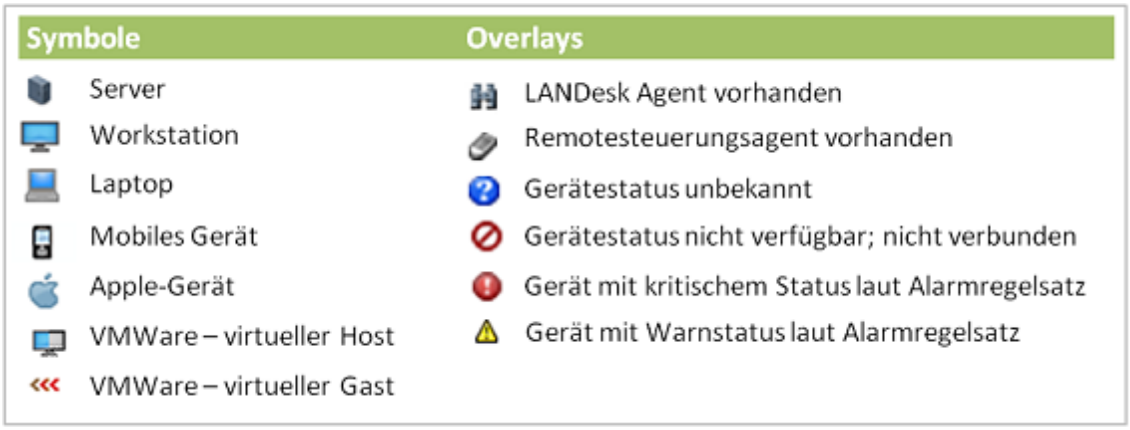
Wenn Sie LANDesk Inspector zum Anzeigen von Daten verwenden, können Sie auf ein Diagramm im Inspector-Fenster klicken und die Details im Fenster **Inspector-Ergebnisse** anzeigen.

Werden die Ergebnisse auf diese Weise angezeigt, können Aktionen für die Daten ausgeführt werden. Beispielsweise kann in einem Diagramm des Inspector für Geplante Tasks angezeigt werden, bei wie vielen Geräten ein Task fehlgeschlagen ist. Wenn Sie auf das Diagramm doppelklicken, sehen Sie die einzelnen Geräte im Order **Inspector-Ergebnisse** aufgelistet. Sie können dann eine Aktion auf diese Geräte anwenden (z. B. den Task neu starten) oder einen Bericht mit den entsprechende Daten anzeigen, sodass Sie nachfassen können.

Die Daten im Order **Inspector-Ergebnisse** ändern sich jedes Mal, wenn Sie in einem Inspector-Fenster auf ein Diagramm klicken.

Netzwerkansicht-Symbole

In der Netzwerkansicht wird neben jedem Element in der Ergebnisliste ein Symbol angezeigt, anhand dessen der Gerätetyp identifiziert werden kann. Je nachdem, welcher Agent installiert ist, welches Gerät momentan angeschlossen ist, welcher Zustandsstatus gegeben ist usw., kann auch eine kleine Symbolüberlagerung auf oder neben dem Gerätesymbol erscheinen, nachdem Sie darauf geklickt haben.

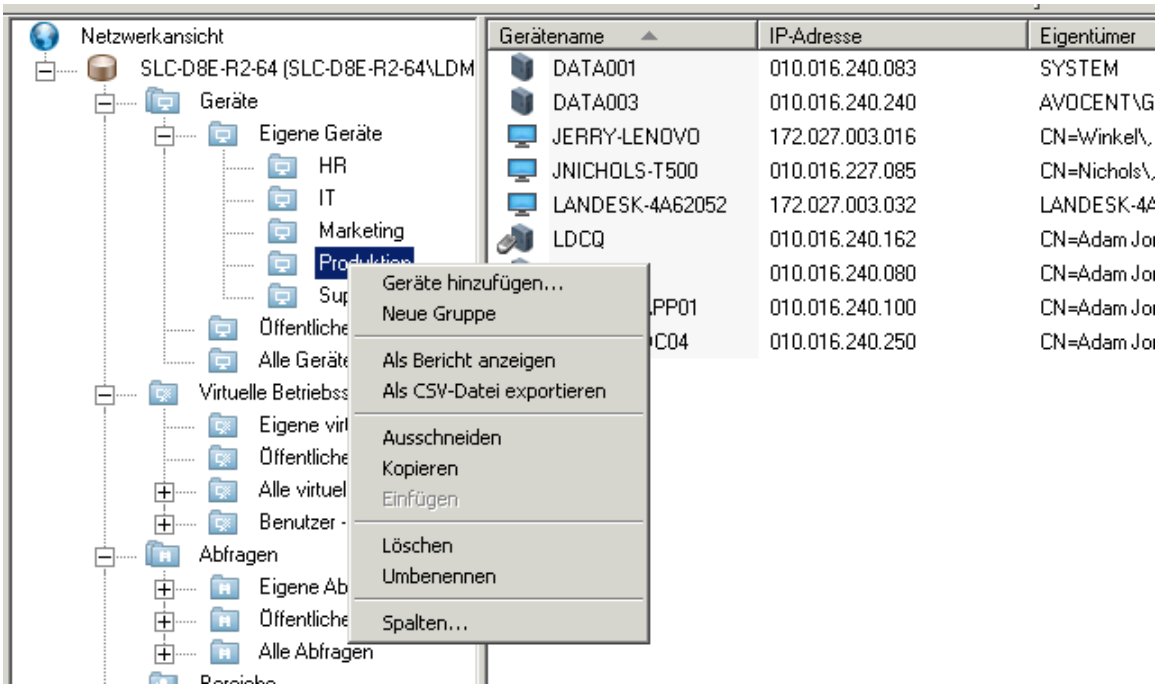


Sie können den Agenten und Systemzustand jeweils für ein Gerät aktualisieren, indem Sie das Gerät in der Netzwerkansicht auswählen. Es können jedoch auch alle in der Netzwerkansicht angezeigten Geräte gleichzeitig aktualisiert werden. Sie können den Status eines Geräts auch aktualisieren, indem Sie ihn auswählen und in der Symbolleiste auf "Aktualisieren" klicken. Informationen über die Konfiguration der Agentenerkennung finden Sie unter "Konfigurieren der Agentenerkennung" auf Seite 105.

HINWEIS: Anzeigequalität der Symbole
Für diese High-Color-Symbole ist eine Farbtiefeneinstellung von mindestens 16 Bit erforderlich. Wenn die Symbole in der Konsole unscharf dargestellt werden, ändern Sie die Farbeinstellungen in den Anzeigeeigenschaften von Windows.

Erstellen von Gruppen in der Netzwerkansicht

Gruppen dienen dazu, Geräte und Abfragen in der Netzwerkansicht der Konsole übersichtlich zusammenzustellen. Sie können Gruppen erstellen, um Netzwerkgeräte nach Funktion, geographischer Lage, Abteilung, Geräteattribut oder einer anderen Kategorie zu ordnen, die Ihren Anforderungen entspricht. Sie können z. B. eine Marketinggruppe für alle Geräte in der Marketingabteilung erstellen oder alle Geräte mit einem bestimmten Betriebssystem zu einer Gruppe zusammenfassen.



Richtlinien für das Erstellen von Gruppen

- **"Eigene Geräte" und "Eigene Abfragen":** Administratoren und alle anderen Benutzer können Gruppen unter **Eigene Geräte** und **Eigene Abfragen** erstellen.
- **Öffentliche Geräte:** Nur Administratoren können Gruppen unter **Öffentliche Geräte** erstellen.
- **Öffentliche Abfragen:** Nur Administratoren oder Benutzer mit dem Recht "Verwaltung öffentlicher Abfragen" können Gruppen unter **Öffentliche Abfragen** erstellen.
- **"Alle Geräte" und "Alle Abfragen":** Es gibt keine Untergruppen für **Alle Geräte** oder **Alle Abfragen**. Benutzer, einschließlich Administratoren, können keine Gruppen unter **Alle Geräte** oder **Alle Abfragen** erstellen.

So erstellen Sie eine Gruppe

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf die übergeordnete Gruppe (z. B. **Eigene Geräte**) und klicken Sie dann auf **Neue Gruppe**. Wählen Sie alternativ die übergeordnete Gruppe aus und klicken Sie dann auf **Bearbeiten** > **Eigene Geräte** > **Neue Gruppe**.
2. Geben Sie einen Namen für die neue Gruppe ein und drücken Sie die **Eingabetaste**.

Kontextmenüs für Gruppen

Sie können mit der rechten Maustaste auf Gruppen klicken, um unterschiedliche Tasks - abhängig vom Gruppentyp - zu erledigen. Wenn Sie beispielsweise eine Geräteuntergruppe erstellt haben, können Sie im Kontextmenü dieser Untergruppe auf mehrere Optionen zugreifen.

- Geräte hinzufügen
- Neue Gruppe (eine neue Untergruppe erstellen)
- Als Bericht anzeigen
- Als CSV-Datei exportieren
- Ausschneiden

- Kopieren
- Einfügen
- Löschen
- Umbenennen
- Spalten (Spalten auswählen, die angezeigt werden sollen)

Weitere Informationen über die Funktionen, die durch Klicken mit der rechten Maustaste angezeigt werden, finden Sie unter "Kontextmenüs" auf Seite 28.

Konfigurieren der Netzwerkansicht mithilfe von Spaltensätzen

Mit Spaltensätzen können Sie die im rechten Fensterausschnitt der Netzwerkansicht eingeblendeten Inventardaten sowohl für Gerätelisten als auch für Listen mit Abfrageergebnissen Ihren Vorstellungen entsprechend ordnen. Jede Spalte in einem Spaltensatz stellt ein eindeutiges Attribut (oder eine eindeutige Komponente) aus dem gescannten Inventar dar. Beispiel: Der Standardspaltensatz der Netzwerkansicht besteht aus den Attributen "Gerätename", "Typ" und "Betriebssystemname".

Erstellen Sie mit dem Extra "Spaltensatzkonfiguration" (**Extras > Administration > Spaltensatzkonfiguration**) die erforderliche Anzahl von Spaltensätzen. Um einen Spaltensatz anzuwenden, ziehen Sie dann den gewünschten Spaltensatz auf Gerätegruppen und Abfrageobjekte in der Netzwerkstrukturansicht.

Das Extra "Spaltensätze"

Im Extra "Spaltensätze" werden Spaltensätze drei Kategorien zugeordnet:

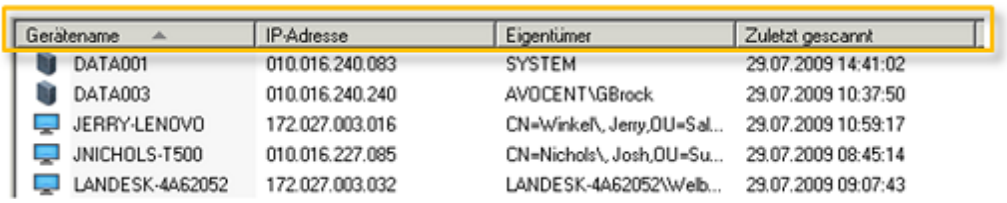
- **Eigene Spaltensätze:** Spaltensätze, die vom aktuell angemeldeten Benutzer erstellt wurden.
- **Öffentliche Spaltensätze:** Von einem Administrator erstellte oder vordefinierte Spaltensätze.
- **Alle Spaltensätze** (nur für den Administrator sichtbar): Spaltensätze, die von allen LANDesk Benutzern erstellt wurden.

Benutzer können einen Spaltensatz aus der Gruppe "Öffentliche Spaltensätze" in ihre eigene Gruppe "Eigene Spaltensätze" kopieren und dann die Spaltensatzeigenschaften anpassen.

Sie können Untergruppen unter dem Objekt **Eigene Spaltensätze** erstellen, um Ihre Spaltensätze zusätzlich zu ordnen.

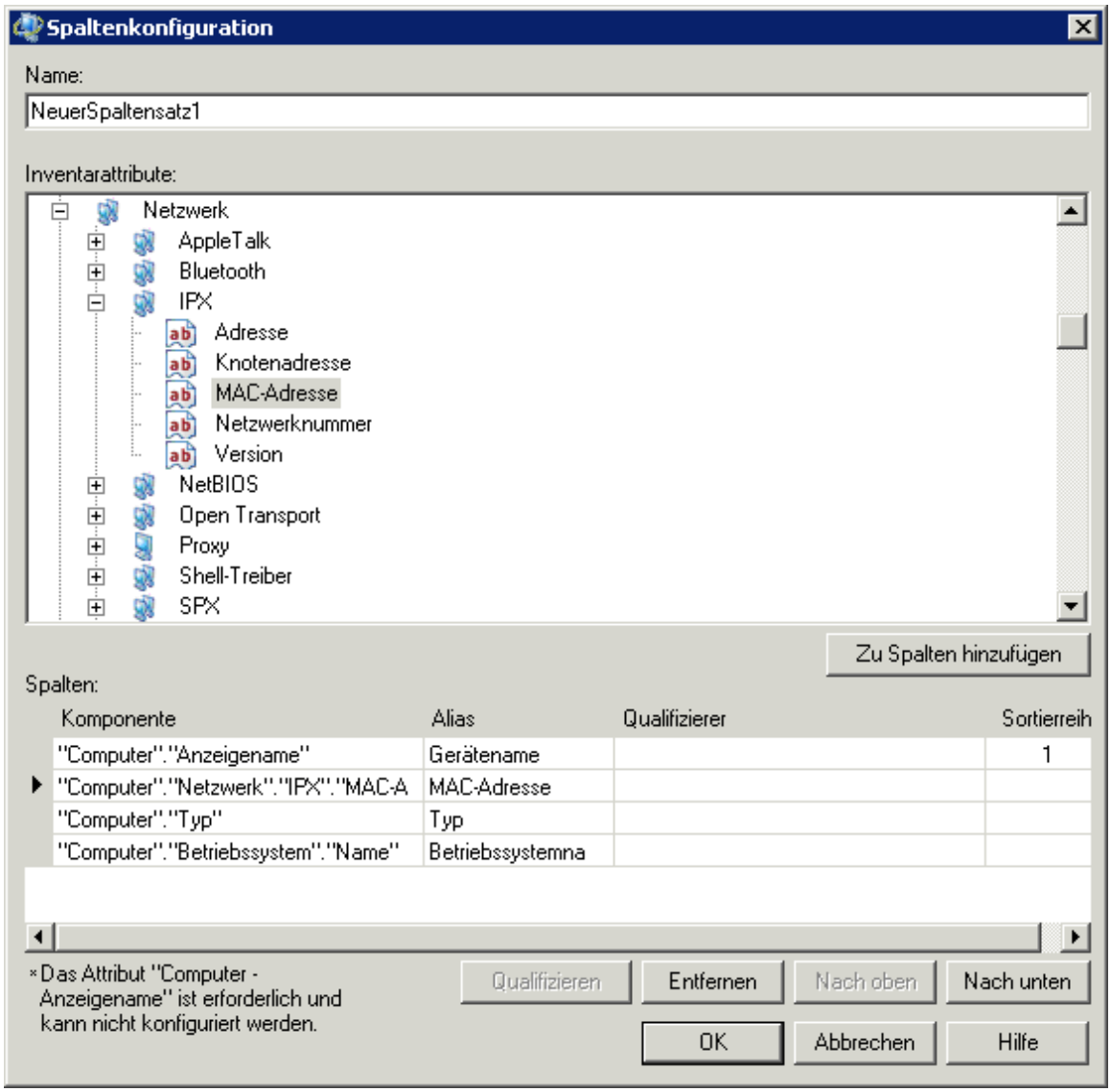
Erstellen von Spaltensätzen

Spaltensätze werden im Dialogfeld **Spaltenkonfiguration** erstellt. Jede Spalte entspricht einem einzelnen Inventarattribut oder einer Komponente, das/die in die Coredatenbank gescannt wurde. Spalten werden in der Netzwerkansicht von links nach rechts angezeigt.. Wenn Sie einen Spaltensatz erstellen oder bearbeiten, können Sie die Attribute angeben, die Sie einschließen möchten.



So erstellen Sie einen Spaltensatz

1. Klicken Sie auf **Extras > Administration > Spaltensatzkonfiguration**.
2. Wählen Sie das Objekt **Eigene Spaltensätze** (oder **Öffentliche Spaltensätze**) aus und klicken Sie dann in der Symbolleiste auf die Schaltfläche **Einen neuen Spaltensatz erstellen**.
3. Geben Sie im Dialogfeld **Spaltenkonfiguration** einen Namen für den neuen Spaltensatz ein.



4. Wählen Sie Inventarattribute aus der Liste aus und fügen Sie sie der Liste "Spalten" hinzu, indem Sie auf **Zu Spalten hinzufügen** klicken. Wählen Sie dabei Attribute aus, die Ihnen helfen, die in der Geräteliste enthaltenen oder von der Abfrage zurückgegebenen Geräte zu identifizieren.

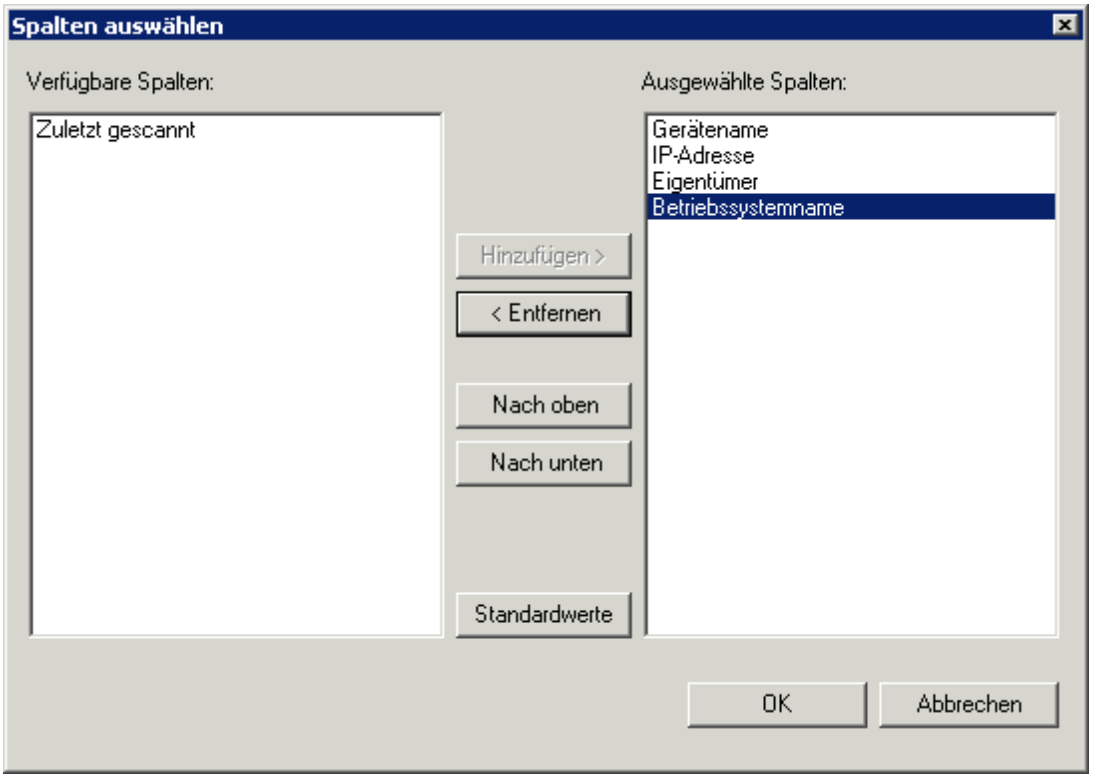
5. (Optional) Sie können festlegen, wie und wo die Spalten in der Netzwerkansicht angezeigt werden. Hierfür müssen Sie entweder die Überschrifts-, Alias- und Sortierfolgefelder einer Komponente direkt bearbeiten oder die ausgewählte Komponente mit den verfügbaren Schaltflächen aus der Liste entfernen oder nach oben oder unten verschieben.
6. (Optional) Sie können noch genauer qualifizierte Daten für Softwarekomponenten angeben. Wählen Sie die Softwarekomponente aus, klicken Sie auf die Schaltfläche **Qualifizieren** und wählen Sie den primären Schlüsselwert aus der Liste der verfügbaren Werte aus. Weitere Informationen finden Sie unter "Angeben der Option "Qualifizieren" bei Softwarekomponenten" auf Seite 17.
7. Klicken Sie auf **OK**, um den Spaltensatz zu speichern.

Spaltenanzeige

Wenn Sie bestimmte Inventarattribute definiert haben und dann entscheiden, dass Sie eine Spalte ausblenden oder deren Position in der Netzwerkansicht ändern möchten, können Sie das Startmenü verwenden, um das Dialogfeld **Spalten auswählen** aufzurufen.

So ändern Sie angezeigte Spalten oder blenden diese aus:

1. Klicken Sie mit der rechten Maustaste auf ein beliebiges Gerät in der Ergebnisliste der Netzwerkansicht.
2. Wählen Sie **Spalten...** aus.
3. Verwenden Sie die Schaltflächen **Hinzufügen >**, **< Entfernen**, **Nach oben** oder **Nach unten**, um die Spalten anzuordnen.
4. Klicken Sie auf **OK**.



Sie können auch zur ursprünglichen Konfiguration der Spaltenanzeige zurückzukehren, indem Sie auf **Standardwerte** klicken.

Übernehmen von Spaltensätzen für Gerätegruppen und Abfragen

Sie können einen fertig gestellten Spaltensatz in eine Gerätegruppe oder Untergruppe oder zu einem bestimmten Abfrageobjekt in einer Abfragegruppe oder Untergruppe ziehen. In der Geräteliste oder Liste mit den Abfrageergebnissen werden die Inventardaten eingeblendet, die von dem ausgewählten Spaltensatz im rechten Fensterausschnitt der Netzwerkansicht angegeben wurden.

Beachten Sie bei Gerätelisten Folgendes: Sobald ein Spaltensatz auf eine Gruppe angewendet wurde, wird diese Einstellung übernommen, selbst wenn Sie andere Gerätegruppen auswählen. Im Gegensatz dazu muss bei Listen mit Abfrageergebnissen der Spaltensatz bei einem Wechsel zu anderen Abfragen neu übertragen werden.

Sie können auch mit der rechten Maustaste auf einen Spaltensatz klicken und über das Kontextmenü globale Tasks ausführen sowie Eigenschaften anzeigen und bearbeiten. Das Kontextmenü umfasst folgende Optionen:

- Zu neuer Gruppe hinzufügen
- Zur vorhandenen Gruppe hinzufügen
- Gruppenmitgliedschaft
- Als Standard festlegen
- Als Bericht anzeigen
- Als CSV-Datei exportieren
- Kopieren
- Löschen
- Umbenennen
- Eigenschaften
- Info
- Exportieren
- Auf anderen Core bzw. andere Cores kopieren
- Automatische Synchronisierung
- Spalten

Angeben der Option "Qualifizieren" bei Softwarekomponenten

Beim Erstellen von Spaltensätzen, die Softwarekomponenten einschließen, können Sie einen Qualifizierer für die betreffenden Softwarekomponenten angeben, indem Sie einen bestimmten primären Schlüsselwert auswählen. Mit einem Softwarequalifizierer können Sie die Daten genauer beschreiben, nach denen eine Abfrage suchen soll und die in der Spalte dieser Softwarekomponente angezeigt werden sollen. Sie können den Spaltensatz z. B. so konfigurieren, dass Versionsdaten nur für eine bestimmte Anwendung angezeigt werden, indem Sie den Namen der ausführbaren Datei dieser Anwendung als Qualifizierer auswählen.

Um den Qualifizierer einer Softwarekomponente anzugeben, wählen Sie die Softwarekomponente in der Liste "Spalten" aus, klicken auf die Schaltfläche **Qualifizieren** und wählen dann einen Wert aus der Liste mit den verfügbaren primären Schlüsselwerten aus.

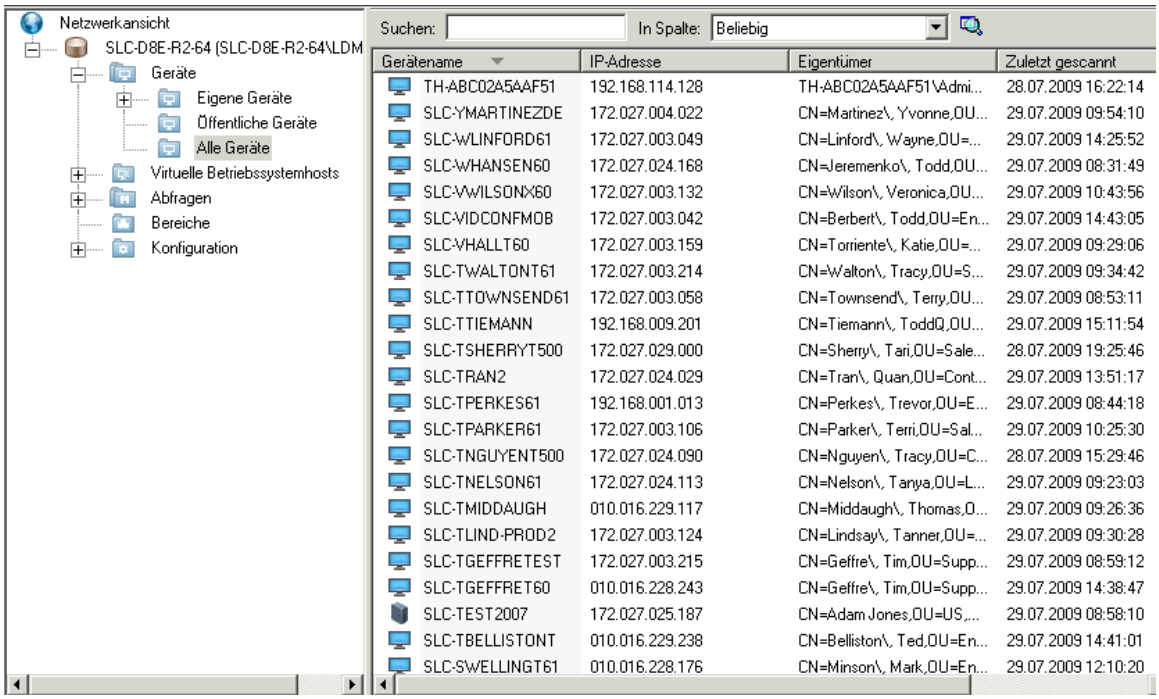
Informationen zum Dialogfeld "Spaltenkonfiguration"

Dieses Dialogfeld enthält folgende Optionen:

- **Name:** Identifiziert die Spaltenkonfiguration.
- **Inventarattribute:** Listet alle Inventarobjekte und die Attribute auf, die in die Coredatenbank gescannt wurden. Sie können Objekte erweitern oder reduzieren, indem Sie auf das Feld links vom Objekt klicken.
- **Zu Spalten hinzufügen:** Verschiebt das ausgewählte Inventarattribut in die Spaltenliste. Wenn Sie eine ganze Inventarkomponente auswählen, werden alle Inventarattribute in dieser Komponente zur Liste "Spalten" hinzugefügt.
- **Spalten:** Führt die Inventarattribute in der Reihenfolge auf, in der sie in der Netzwerkansicht angezeigt werden; von links nach rechts.
- **Qualifizieren:** Hiermit können Sie einen exakten Datenqualifizierer für die ausgewählte Softwarekomponente angeben. Weitere Informationen finden Sie unter "Angeben der Option "Qualifizieren" bei Softwarekomponenten" auf Seite 17.
- **Entfernen:** Entfernt das ausgewählte Attribut aus der Liste.
- **Nach oben:** Verschiebt das ausgewählte Attribut um eine Position nach oben.
- **Nach unten:** Verschiebt das ausgewählte Attribut um eine Position nach unten.
- **OK:** Speichert die aktuelle Spaltenkonfiguration und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Anzeigen von erkannten Geräten

Geräte, die LANDesk-Agenten automatisch ausführen, werden in der Gruppe **Alle Geräte** angezeigt, sobald sie vom Inventarscanner in die Coredatenbank gescannt werden. In der Regel wird dieser Scan zum ersten Mal während der ersten Agentenkonfiguration eines Geräts durchgeführt. Ein Gerät, das gescannt und dessen Inventarbericht an die Coredatenbank gesendet wurde, ist ein verwaltetes Gerät. Mit anderen Worten, es kann jetzt von diesem Coreserver verwaltet werden. Weitere Informationen zum Einrichten von Geräten finden Sie unter "Agentenkonfiguration" auf Seite 105.

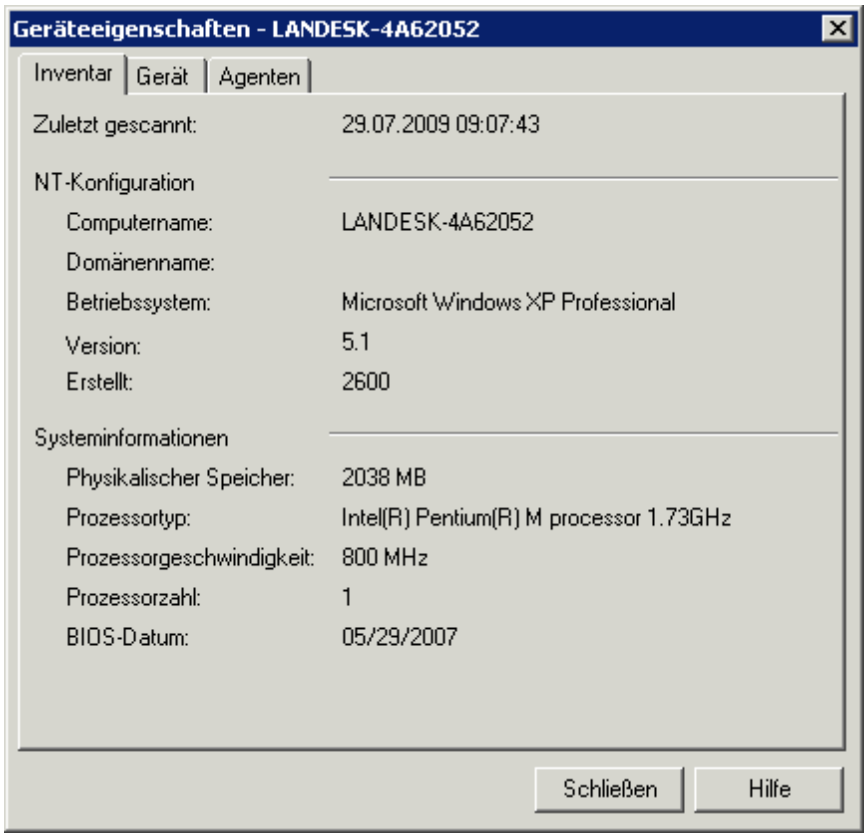

Netzwerkansicht
SLC-D8E-R2-64 (SLC-D8E-R2-64\LDM
Geräte
Eigene Geräte
Öffentliche Geräte
Alle Geräte
Virtuelle Betriebssystemhosts
Abfragen
Bereiche
Konfiguration
Suchen:
In Spalte: Beliebig
Gerätename
IP-Adresse
Eigentümer
Zuletzt gescannt
TH-ABC02A5AAF51 192.168.114.128 TH-ABC02A5AAF51\Admi... 28.07.2009 16:22:14
SLC-YMARTINEZDE 172.027.004.022 CN=Martinez\, Yvonne,OU... 29.07.2009 09:54:10
SLC-WLINFORD61 172.027.003.049 CN=Linford\, Wayne,OU=... 29.07.2009 14:25:52
SLC-WHANSEN60 172.027.024.168 CN=Jeremenko\, Todd,OU... 29.07.2009 08:31:49
SLC-VWILSONX60 172.027.003.132 CN=Wilson\, Veronica,OU... 29.07.2009 10:43:56
SLC-VIDCONFMOB 172.027.003.042 CN=Berbert\, Todd,OU=En... 29.07.2009 14:43:05
SLC-VHALLT60 172.027.003.159 CN=Torriente\, Katie,OU=... 29.07.2009 09:29:06
SLC-TWALTONT61 172.027.003.214 CN=Walton\, Tracy,OU=S... 29.07.2009 09:34:42
SLC-TTOWNSEND61 172.027.003.058 CN=Townsend\, Terry,OU... 29.07.2009 08:53:11
SLC-TTIEMANN 192.168.009.201 CN=Tiemann\, ToddQ,OU... 29.07.2009 15:11:54
SLC-TSHERRYT500 172.027.029.000 CN=Sherry\, Tari,OU=Sale... 28.07.2009 19:25:46
SLC-TRAN2 172.027.024.029 CN=Tran\, Quan,OU=Cont... 29.07.2009 13:51:17
SLC-TPERKES61 192.168.001.013 CN=Perkes\, Trevor,OU=E... 29.07.2009 08:44:18
SLC-TPARKER61 172.027.003.106 CN=Parker\, Terri,OU=Sal... 29.07.2009 10:25:30
SLC-TNGUYENT500 172.027.024.090 CN=Nguyen\, Tracy,OU=C... 28.07.2009 15:29:46
SLC-TNELSON61 172.027.024.113 CN=Nelson\, Tanya,OU=L... 29.07.2009 09:23:03
SLC-TMIDDAUGH 010.016.229.117 CN=Middaugh\, Thomas,O... 29.07.2009 09:26:36
SLC-TLIND-PROD2 172.027.003.124 CN=Lindsay\, Tanner,OU=... 29.07.2009 09:30:28
SLC-TGEFFRETEST 172.027.003.215 CN=Geffre\, Tim,OU=Supp... 29.07.2009 08:59:12
SLC-TGEFFRET60 010.016.228.243 CN=Geffre\, Tim,OU=Supp... 29.07.2009 14:38:47
SLC-TEST2007 172.027.025.187 CN=Adam Jones,OU=US,... 29.07.2009 08:58:10
SLC-TBELLISTONT 010.016.229.238 CN=Belliston\, Ted,OU=En... 29.07.2009 14:41:01
SLC-SWELLINGT61 010.016.228.176 CN=Minson\, Mark,OU=En... 29.07.2009 12:10:20

Da die Gruppe **Alle Geräte** automatisch mithilfe eines Inventarscans gefüllt wird, müssen Sie möglicherweise nie manuell nach Geräten suchen. Um jedoch Geräte zu finden, die sich nicht bereits in der Coredatenbank befinden, können Sie das Netzwerk mit dem Extra "Erkennung nicht verwalteter Geräte" nach Geräten durchsuchen lassen. Nähere Informationen finden Sie unter "Anzeigen einer Inventarübersicht" auf Seite 158.

Wenn eine Verbindung zu einem bestimmten Coreserver besteht, kann der Administrator jedes Gerät sehen, das von diesem Coreserver verwaltet wird. Andere Benutzer sind eingeschränkt und sehen nur die Geräte, die zu dem ihnen zugewiesenen Bereich gehören (ein Bereich basiert auf einer Datenbankabfrage oder einem Verzeichnisstandort). Weitere Informationen finden Sie unter "Benutzerverwaltung" auf Seite 40.

Anzeigen von Geräteeigenschaften

In der Netzwerkansicht der Konsole können Sie in kürzester Zeit Informationen zu einem Gerät anzeigen, indem Sie in der Geräteliste mit der rechten Maustaste auf das Gerät klicken und **Eigenschaften** auswählen.



Das Dialogfeld "Geräteeigenschaften"

In diesem Dialogfeld können Sie nützliche Informationen über das ausgewählte Gerät anzeigen. Das Dialogfeld umfasst drei Registerkarten: **Inventar**, **Gerät** und **Agenten**. Klicken Sie auf die jeweilige Registerkarte, um die entsprechenden Informationen anzuzeigen.

Informationen zur Registerkarte "Inventar"

Die Registerkarte **Inventar** enthält eine Zusammenfassung der Inventardaten des Geräts. Nähere Informationen finden Sie unter "Anzeigen einer Inventarübersicht" auf Seite 158.

Registerkarte "Gerät"

Die Registerkarte **Gerät** enthält die wichtigsten Informationen zu einem bestimmten Gerät, einschließlich dessen Speicherort und Identität im Netzwerk. Diese Registerkarte wird auch angezeigt, wenn Sie ein Gerät manuell hinzufügen (im Kontextmenü der Gruppe **Alle Geräte** auf **Neuen Computer einfügen** klicken).

- **Gerät:**
  - **Name:** Der Name, der in der Coredatenbank und in der Netzwerkansicht für dieses Gerät angezeigt wird.
    Wenn Sie ein Gerät manuell hinzufügen, können Sie einen benutzerfreundlichen Namen wählen. Wenn Sie hier nichts eingeben, wird als Standardgerätename der Windows-Computername gewählt.
  - **Typ:** Der Gerätetyp, beispielsweise Windows 2008 Server oder XP Workstation.
- **Netzwerk:**

- **IP-Name:** Der Windows-Computername für das Gerät.
- **IP-Adresse:** Die dem Gerät zugewiesene IP-Adresse.
- **Physikalische Adresse:** Die physikalische Adresse des Geräts.

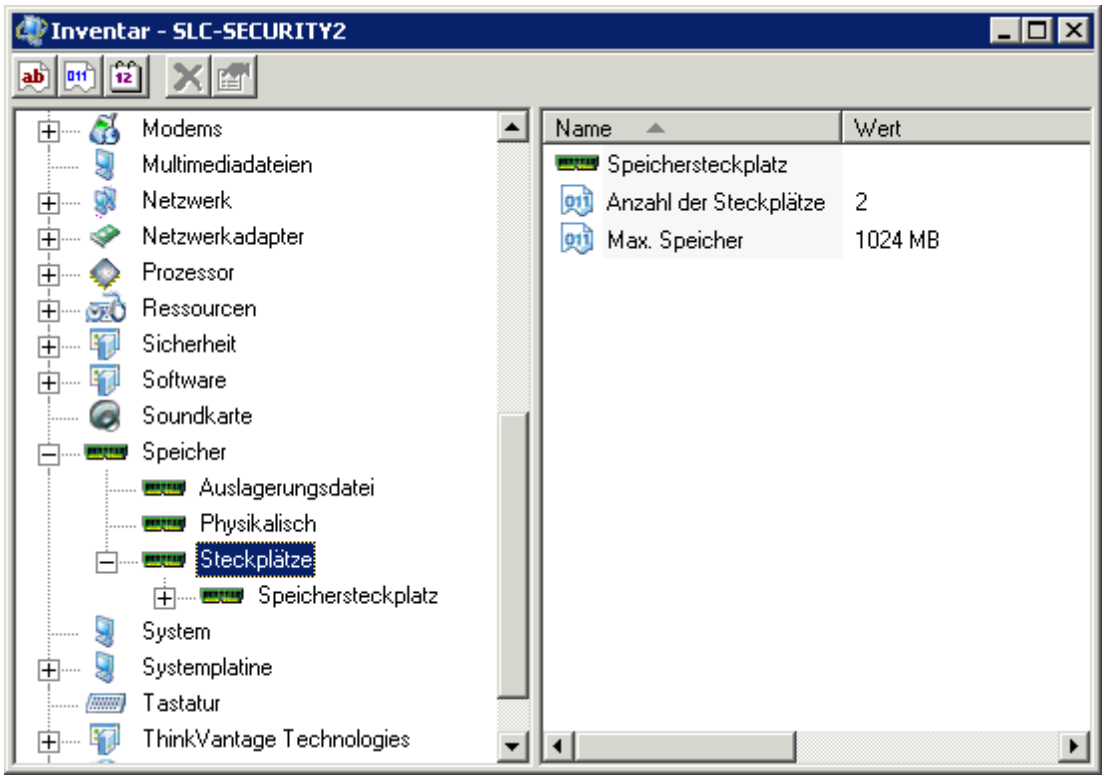
Informationen zur Registerkarte "Agenten"

Die Registerkarte **Agenten** enthält Informationen zum aktuellen Status von Agenten und zu den Remotesteuerungseinstellungen des Geräts.

- **Common Base Agent-Status:** Gibt an, ob der Standard LANDesk Agent (Common Base Agent) auf dem Gerät geladen ist.
- **Echtzeitinventar und Überwachung:** Zeigt an, ob der Agent für Echtzeitinventar und Überwachung auf dem Gerät installiert ist.
- **Remotesteuerungsagenten-Status:** Gibt an, ob der Remotesteuerungsagent auf dem Gerät installiert ist. Wenn dieser Agent nicht auf dem Gerät installiert ist, sind Remotesteuerungsvorgänge (wie Dateitransfer und Chat) nicht verfügbar.
- **Sicherheitstyp:** Zeigt das für das Gerät verwendete Remotesteuerungs-Sicherheitsmodell an. Zu den Optionen gehören: Lokale Vorlage, Windows NT-Sicherheit/lokale Vorlage und zertifikatsbasierte/lokale Vorlage.
- **Zulassen:** Zeigt die Remotesteuerungsvorgänge an, die auf dem Gerät unterstützt werden. Diese Vorgänge wurden durch die Konfiguration des Geräteagenten aktiviert.
- **Einstellungen:** Gibt an, wie die Remotesteuerung reagiert, wenn Sie versuchen, mit dem Gerät zu kommunizieren.

Inventardaten

Genauere Informationen über das Gerät finden Sie in den Inventardaten des Geräts. Sie können umfassende Inventarinformationen anzeigen, indem Sie im Ergebnisbereich der Netzwerkansicht auf den Gerätenamen doppelklicken.



Konfigurieren von Geräteüberwachungsalarmen

Damit Sie von der Geräteüberwachung benachrichtigt werden, wenn verwaltete Geräte online oder offline gehen, müssen Sie zuerst einen Alarmregelsatz mit zusätzlichen Aktionen konfigurieren (wie z. B. Empfang einer E-Mail, wenn ein Alarm gesendet wird).

So konfigurieren Sie Alarmeinstellungen für die Geräteüberwachung

1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Erweitern Sie im Baum **Alarme** das Element **Alarmregelsätze**.
3. Klicken Sie mit der rechten Maustaste auf **Core-Alarmregelsätze** und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie im Fenster **Regelsatz** im Bereich **Alarmregelsatz** auf **Alarme**.
5. Klicken Sie im Bereich **Alarme** unter dem Order **Standard** auf **Geräteüberwachung**.
6. Klicken Sie im rechten Fensterausschnitt auf **Regeln > Hinzufügen**.
7. Ziehen Sie den Alarm **Geräteüberwachung – Systemkonnektivität** auf den Auswahlbereich **Alarme** am unteren Rand der Seite.
8. Klicken Sie im Fenster **Regelsatz** im Bereich **Alarmregelsatz** links auf **Aktionen** und ziehen Sie beliebige zusätzliche Regelsätze nach unten auf den Auswahlbereich **Aktionen**. Die Core-Alarmprotokoll-Handlerkonfiguration bildet die standardmäßige Aktion. Sie können entscheiden, ob Sie beim Empfang eines Alarms eine E-Mail oder einen SNMP-Trap senden oder eine ausführbare Datei auf dem Core ausführen möchten. (Unter Umständen müssen Sie jede Aktion definieren, z. B. angeben, wohin die E-Mail-Alarme gesendet werden sollen.)

9. Klicken Sie im Fenster **Regelsatz** links im Bereich **Alarmregelsatz** auf **Zeit** und ziehen Sie **Immer** nach unten auf den Auswahlbereich **Zeit**.
10. Klicken Sie neben den Auswahlbereichen auf die Schaltfläche **OK**.
11. Klicken Sie im rechten Fensterausschnitt **Aktionen** auf **Veröffentlichen**.
12. Klicken Sie im linken Fensterbereich **Alarmregelsatz** auf **Regelübersicht** und doppelklicken Sie dann auf die von Ihnen erstellte Regel.
13. In dem daraufhin angezeigten Dialogfeld markieren Sie das Kontrollkästchen **Zustand**, wenn sich der Gerätezustand in der Konsole ändern soll, je nachdem, ob da Gerät online oder offline ist. Klicken Sie dann auf **OK**, um das Dialogfeld zu schließen.
14. Klicken Sie auf **Veröffentlichen**, um alle Änderungen zu veröffentlichen, die Sie in dem Dialogfeld vorgenommen haben und das Dialogfeld **Regelsatz** zu schließen.

HINWEIS: Wenn Sie Alarmeinstellungen konfigurieren, werden diese auf alle von Ihnen überwachten Geräte angewendet.

Überwachen von Geräten auf Netzwerkkonnektivität

Mithilfe der Geräteüberwachung können Sie regelmäßig die Konnektivität der verwalteten Geräte überwachen.

Die Pingeinstellungen gelten speziell für das Gerät, das Sie ausgewählt haben. Wenn ein Gerät nicht mehr auf einen Ping reagiert (also offline ist) wird eine Alarmbenachrichtigung zum Protokoll auf dem Coreserver hinzugefügt. Wenn Sie durch eine andere Alarmaktion benachrichtigt werden wollen, beispielsweise indem Sie eine E-Mail erhalten, wenn ein Gerät offline geht, können Sie einen Alarm im Alarmregelsatz des Cores konfigurieren.

So überwachen Sie die Konnektivität von verwalteten Geräte

1. Klicken Sie auf **Konfigurieren > Geräteüberwachung**.
2. Klicken Sie auf **Hinzufügen**. Wählen Sie ein oder mehrere Geräte aus, die Sie überwachen möchten und klicken Sie dann auf **Hinzufügen**.
3. Definieren Sie die Einstellung der **Pingfrequenz**, die Anzahl der Wiederholungen und das Timeoutlimit.
4. Klicken Sie auf **OK**.

Informationen zum Dialogfeld "Geräteüberwachung konfigurieren"

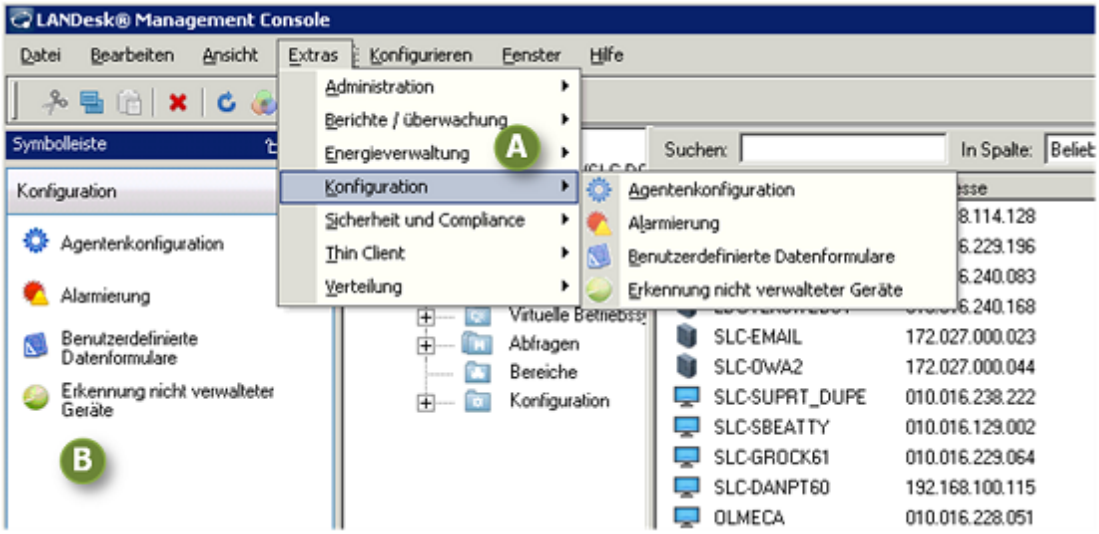
In diesem Dialogfeld können Sie folgende Optionen für die Geräteüberwachung konfigurieren:

- **Diese Geräte überwachen:** Gibt die derzeit überwachten Geräte an.
- **Hinzufügen:** Öffnet das Dialogfeld **Überwachte Geräte hinzufügen**. Dort können Sie nach verwalteten Geräten suchen und verwaltete Geräte aussuchen, die Sie überwachen möchten.
- **Entfernen:** Entfernt das ausgewählte Gerät aus der Liste.
- **Pingfrequenz:** Steuert, wann und wie der Pingvorgang abläuft. Diese Einstellungen können auf jedes Gerät einzeln übertragen werden.
    - **Ping alle:** Plant einen regelmäßigen Ping im festgelegten Minutenintervall.
    - **Täglich planen um:** Plant einen täglichen Ping zu einer festgelegten Zeit.
    - **Versuche:** Legt die Anzahl der Pingwiederholungen fest.

- **Timeout:** Legt die Anzahl der Sekunden fest, bis das Timeout für die Pingwiederholungen eintritt.
- **OK:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Zugriff auf Konsolenextras

Konsolenextras werden sowohl über das Menü "Extras" **(A)** als auch über die Toolbox **(B)** zur Verfügung gestellt. Klicken Sie zum Aktivieren der Toolbox auf **Ansicht > Toolbox**. Um Platz in der Konsole zu sparen, können Sie auch auf die Aktivierung der Toolbox verzichten und einfach Extras aus dem Menü "Extras" auswählen.



***A** Menü "Extras", **B** Toolbox-Bereich*

Der Management Suite Administrator sieht alle Extras, sowohl die im Menü "Extras" als auch die in der **Toolbox**. Andere Management Suite Benutzer sehen nur die Extras und Funktionen, auf die sie aufgrund der ihnen zugewiesenen Rechte Zugriff haben. Extras, deren Verwendung an Rechte geknüpft ist, die einem Benutzer nicht gewährt wurden, werden weder im Menü "Extras" noch in der Toolbox angezeigt, wenn der betreffende Benutzer an der Konsole angemeldet ist. Wenn ein Benutzer z. B. nicht über das Recht "Energieverwaltung" verfügt, wird das Extra "Energieverwaltung" weder im Menü **Extras** noch in der **Toolbox** angezeigt.

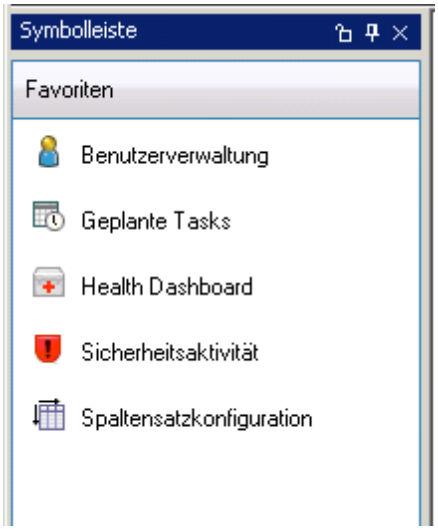
Wenn Sie auf den Namen eines Extras klicken, wird dessen Fenster in der Konsole unterhalb der Netzwerkansicht geöffnet.

Die Fenster der Extras können vergrößert/verkleinert, verankert, unverankert, ausgeblendet und geschlossen sein. Sie können mehrere Extra-Fenster gleichzeitig geöffnet haben, verankert oder unverankert. Weitere Informationen finden Sie unter "Verschieben und Ändern der Größe von Extra-Fenstern" auf Seite 25.

Favoriten

Wenn Sie feststellen, dass Sie bestimmte Extras häufiger als andere verwenden, können Sie schnell und einfach eine Favoriten-Toolbox erstellen, indem Sie mit der rechten Maustaste auf ein beliebiges Extra in der Toolbox klicken und die Option "In Favoriten anzeigen" auswählen. Im Anschluss daran können Sie über die Schaltfläche "Favoriten" unten im Toolbox-Bereich auf Ihre Favoriten zugreifen.

Bild anzeigen/ausblenden



Verschieben und Ändern der Größe von Extra-Fenstern

Sie können in der Konsole beliebig viele Extras öffnen und in das Hauptkonsolenfenster bzw. aus dem Hauptkonsolenfenster verschieben.

HINWEIS: Sie können von Ihnen erstellte Konsolenlayouts, die Sie für bestimmte Verwaltungstasks verwenden möchten, speichern und ein gespeichertes Layout bei Bedarf jederzeit wiederherstellen. Weitere Informationen finden Sie unter "Speichern von Konsolenlayouts" auf Seite 30.

Wenn Sie mehrere Extra-Fenster öffnen, werden diese mit Registerkarten in einem einzelnen Fenster angezeigt. Das aktive Extra-Fenster wird im Vordergrund angezeigt, wobei für jedes geöffnete Extra entlang der Seite oder Unterseite eine Registerkarte eingeblendet wird. Klicken Sie auf eine Registerkarte, um das betreffende Extra-Fenster anzuzeigen.

Verankern von Extra-Fenstern

Ein Extra-Fenster zu verankern bedeutet, es an eine der Kanten der Konsole anzufügen. Das Fenster gilt als verankert, wenn es an eine Kante der Konsole angehängt wurde. Sie können Fenster waagrecht oder senkrecht in der Konsole verankern.

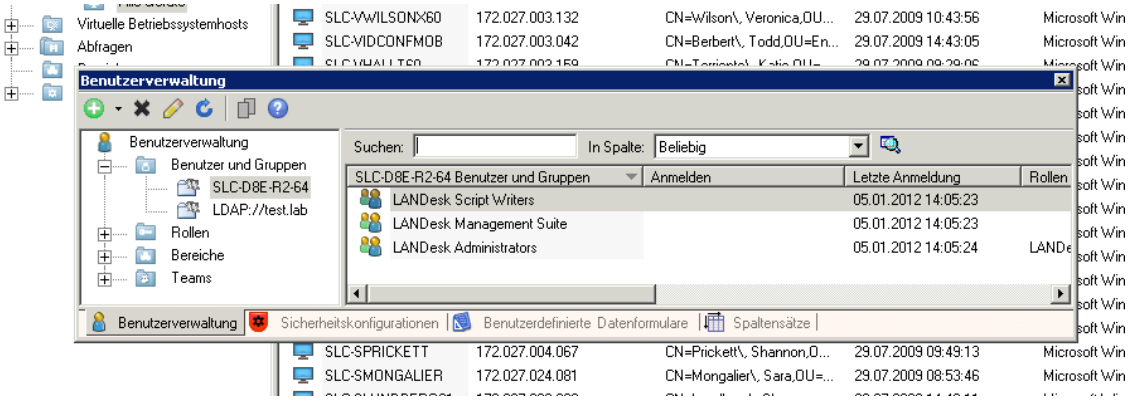
So verankern Sie ein Extra-Fenster

1. Klicken Sie auf die Titelleiste eines Fensters und ziehen Sie das Fenster an eine Kante der Konsole.
2. Wenn das Verankerungsrechteck (abgeblendete Kontur des Fensters) angezeigt wird und signalisiert, dass das Fenster verankert wird, lassen Sie die Maustaste los. Das Fenster wird an diese Kante der Konsole angehängt.

Verankerung von Extra-Fenstern aufheben

Sie können die Verankerung des Extras-Fensters auch aufheben und an der Titelleiste des Fensters ziehen, so dass es unverankert an einen anderen Ort innerhalb oder außerhalb der Konsole verschoben werden kann. Unverankerte Extras können durch Ziehen verschoben bzw. in Ihrer Größe verändert werden, um vorübergehend Platz für die Arbeit mit anderen Tasks zu schaffen. Wenn Sie das Extras-Fenster durch Ziehen verschieben, bewegen sich die Registerkarten aller anderen derzeit geöffneten Extras analog dazu. Um das Extra wieder zurück an seine verankerte bzw. ursprüngliche Position zu bewegen, klicken Sie einfach doppelt darauf. Sie können es aber auch auf seine Position zurückziehen und loslassen, sobald Sie das graue Dockingrechteck an der richtigen Stelle sehen.

Bild anzeigen/ausblenden



Beachten Sie, dass nur Extra-Fenster (über das Menü "Extras" oder die Toolbox verfügbare Fenster) verankert, unverankert oder mit Registerkarten ausgestattet sein können. Das Fenster "Netzwerkansicht" kann vergrößert oder verkleinert werden, es kann jedoch nicht als Registerkarte zusammen mit anderen Fenstern angezeigt oder außerhalb der Konsole frei angeordnet oder geschlossen werden.

Wenn Sie das Hauptfenster der Konsole verkleinern und dann wiederherstellen, werden bei diesem Vorgang alle verankerten und unverankerten Fenster, einschließlich der Fenster mit Registerkarten, ebenfalls verkleinert und wiederhergestellt.

Automatisches ausblenden von Extra-Fenstern

Extra-Fenster unterstützen ferner die Funktion zum automatische Ausblenden. Es handelt sich dabei um eine Schaltfläche in Form einer Stecknadel, die in der oberen rechten Ecke eines Fensters zu sehen ist. Mit der Stecknadel wird das Fenster arretiert oder ausgeblendet.

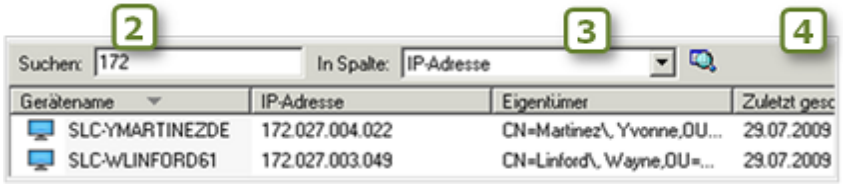
Wenn die Stecknadel eingedrückt ist (d. h. nach unten zeigt), bedeutet dies, dass das Fenster fest an seinem Platz verankert und die Funktion zum automatischen Ausblenden vorübergehend deaktiviert ist. Wenn die Stecknadel nicht eingedrückt ist (d. h. nach links zeigt), wird das Fenster automatisch ausgeblendet, sobald sich der Cursor außerhalb des Fensters befindet. Die Funktion zum automatischen Ausblenden verkleinert das Fenster, verankert es an einer der Kanten der Konsole und zeigt an seiner Stelle eine Registerkarte an.

Der Toolboxbereiche unterstützt die Funktion zum automatische Ausblenden ebenfalls.

Suche nach Elementen mithilfe der Suchleiste

Die Suchleiste wird immer dann in der Symbolleiste angezeigt, wenn es für den Benutzer zweckmäßig ist, in einer entsprechenden Liste nach einem bestimmten Element zu suchen. So wird beispielsweise jedes Mal, wenn eine Liste von Elementen im oberen oder unteren Teil der Konsole angezeigt wird, eine Suchleiste bereitgestellt, mit der ein bestimmtes Element in der entsprechenden Liste gefunden werden kann.

Ein Beispiel hierzu wird im Folgenden gegeben. Nehmen wir an, dass in der Datenbank eines Unternehmens 10.000 Knoten aufgelistet sind. Ein Benutzer bittet um Unterstützung und das Helpdesk-Team muss das Gerät in der Konsole finden. Das Mitglied des Helpdesks kann den Anrufer nach dem Anmeldenamen oder dem Gerätenamen oder anderen benutzer- oder gerätespezifischen Informationen fragen und genau den einen entsprechenden Eintrag unter 10.000 Einträgen in ein oder zwei Sekunden ausfindig machen.



Schritt 2** Textfeld **Suchen**, **3** Liste **In Spalte:**, **4** Schaltfläche **Suchen

So suchen Sie nach einem Element mithilfe der Suchleiste

1. Wählen Sie die Gruppe **Alle Geräte** aus. Die **Suchleiste** wird am Beginn der Liste angezeigt.
2. Geben Sie in das Textfeld **Suchen** einen beliebigen Text ein, nach dem Sie suchen möchten.
3. Wählen Sie in der Liste **In Spalte** die Spalte aus, die Sie durchsuchen möchten.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Suche**.

Die Ergebnisliste zeigt nur die Elemente an, die Ihren Suchkriterien entsprechen.

Symbolleistenoptionen

Die Konsole enthält eine Symbolleiste, über die Sie per Mausklick auf häufig ausgeführte Aktionen in der Netzwerkansicht und auf die wichtigsten Konsolenkonfigurationsoptionen zugreifen können. Die Schaltflächen der Symbolleisten sind abgeblendet, wenn ein Element in der Netzwerkansicht ausgewählt ist, das den betreffenden Vorgang nicht unterstützt.

Symbolleistenschaltflächen der Konsole

- **Ausschneiden:** Entfernt Elemente aus der Netzwerkansicht und speichert sie temporär in der Zwischenablage. Wenn Sie versehentlich ein Element ausschneiden, verwenden Sie die Funktion "Einfügen", um es wiederherzustellen. Sie müssen das gelöschte Element wiederherstellen, bevor Sie einen anderen Befehl ausführen.
- **Kopieren:** Kopiert Elemente von einem Speicherort in der Netzwerkansicht in einen anderen.
- **Einfügen:** Fügt Elemente ein, die Sie ausgeschnitten oder kopiert haben.
- **Löschen:** Löscht das Element permanent. Sie können keine Elemente wiederherstellen, die Sie aus der Netzwerkansicht gelöscht haben.

- **Aktualisieren:** Aktualisiert die ausgewählte Gruppe oder das Element in der Netzwerkansicht. Sie können eine Gruppe auch reduzieren und erweitern, um die Elemente zu aktualisieren. Sie können auch auf **Ansicht > Aktualisieren** klicken, um das gegenwärtig in der Netzwerkansicht ausgewählte Element zu aktualisieren.
- **Bereich aktualisieren:** Aktualisiert die ausgewählte Gruppe bzw. das ausgewählte Element in der Netzwerkansicht basierend auf dem Bereich des angemeldeten Benutzers (wie im Extra "Benutzer" definiert). Bereiche werden aktualisiert, wenn sich Benutzer anmelden oder wenn ein Konsolenbenutzer mit Administratorrechten auf diese Schaltfläche klickt.
- **Layout:** Führt Ihre gespeicherten Fensterlayouts auf. Wählen Sie ein Layout aus der Dropdownliste aus, um diese Layoutkonfiguration für die Konsole wiederherzustellen. Wenn Sie das aktuelle Layout speichern möchten, klicken Sie auf die Schaltfläche **Aktuelles Layout speichern**.
- **Core:** Führt Coreserver auf, mit denen Sie zu einem früheren Zeitpunkt schon einmal eine Verbindung aufgebaut haben (dies ist der Grund dafür, dass diese Server in dieser Liste angezeigt werden). Sie können einen Coreserver aus der Liste auswählen oder den Namen eines Coreservers eingeben und die **Eingabetaste** drücken. Ihr Netzwerk wird auf diesen Coreserver durchsucht. Wird er gefunden, so werden Sie aufgefordert, sich unter Angabe eines gültigen Benutzernamens und Kennwortes anzumelden.

Kontextmenüs

Für alle Elemente in der Konsole, einschließlich Gruppen, Geräte, Abfragen, geplante Tasks, Skripte, Berichte usw., stehen Kontextmenüs (Shortcut-Menüs) zur Verfügung. Kontextmenüs ermöglichen den schnellen Zugriff auf die allgemeinen Tasks und wichtigen Informationen eines Elements.

Sie können das Kontextmenü eines Elements anzeigen, indem Sie das Element auswählen und mit der rechten Maustaste darauf klicken.

Verfügbare Optionen im Kontextmenü

Die Optionen, die im Kontextmenü des Geräts angezeigt werden, sowie deaktivierte oder abgeblendete Optionen, können je nach Geräteplattform und je nachdem, welche LANDesk Agenten auf dem Gerät installiert sind, voneinander abweichen.

Wenn Sie beispielsweise in der Netzwerkansicht mit der rechten Maustaste auf ein verwaltetes Gerät klicken, zeigt dessen Kontextmenü in der Regel folgende Optionen an:

- **Inventar:** Zeigt alle in die Coredatenbank gescannten Inventardaten des Geräts an.
- **Inventarverlauf:** Zeigt Änderungen der Inventardaten für die Attribute an, die Sie für das Verfolgen ausgewählt haben. Sie können den Inventarverlauf drucken oder in eine CSV-Datei exportieren.
- **Remotesteuerung:** Öffnet eine Remotesteuerungssitzung mit dem Gerät.
    - **Chat:** Öffnet eine Remote-Chatsitzung mit dem Gerät.
    - **Dateiübertragung:** Öffnet das Dialogfeld "Dateiübertragung", das Sie beim Transfer von Dateien auf und von Geräten unterstützt.
    - **Remoteausführung:** Damit können Sie zu einer Batchdatei oder einer Anwendung auf dem Gerät navigieren.
    - **Neu starten:** Ermöglicht es Ihnen, das Gerät neu zu starten.
- **Reaktivieren:** Reaktiviert über Remotezugriff ein Gerät, dessen BIOS die Wake on LAN-Technologie unterstützt.
- **Herunterfahren:** Schaltet das Gerät remote ab.

- **Inventarscan:** Führt einen Inventarscan auf dem Gerät aus.
- Gerätevariablen verwalten:
- Versorgungsverlauf:
- **Geplante Tasks und Richtlinien:** Zeigt die für das Gerät aktuell geplanten Tasks und Anwendungsverwaltungsrichtlinien an.
- **Zu neuer Gruppe hinzufügen:** Fügt eine Kopie des Geräts in eine neue benutzerdefinierte Gruppe unter **Eigene Geräte** ein. Sie werden aufgefordert, einen Namen für die neue Gruppe einzugeben.
- **Zur vorhandenen Gruppe hinzufügen:** Damit können Sie die Gruppe auswählen, der Sie eine Kopie des Geräts hinzufügen möchten.
- **Gruppenmitgliedschaft:** Zeigt alle Gruppen an, denen das Gerät gegenwärtig angehört.
- **Inventarbericht ausführen:** Öffnet das Dialogfeld "Berichte". In diesem Dialogfeld können Sie aus einer entsprechenden Liste die Berichte auswählen, die Sie auf dem Gerät ausführen möchten. Doppelklicken Sie auf einen Berichtsnamen, um den Bericht auszuführen.
- **Agentenüberwachungseinstellungen aktualisieren:** Öffnet das Dialogfeld "Agentenüberwachungseinstellungen aktualisieren". In diesem Dialogfeld können Sie die Echtzeitüberwachung bestimmter LANDesk Agenten und Dienste aktivieren/deaktivieren, eine Agentenüberwachungseinstellung auswählen oder eine neue konfigurieren und ein Zeitintervall für das Scannen auf Änderungen in der ausgewählten Einstellung angeben.
- **Sicherheits- und Patchinformationen:** Ruft das Dialogfeld "Sicherheits- und Patchinformationen" auf, das detaillierte Informationen zu Anfälligkeitsscans und Reparaturen anzeigt, einschließlich erkannten Anfälligkeiten und anderen Sicherheitsrisiken, installierten Patches und Reparaturverlauf.
- **Sicherheits-/Compliancescan:** Öffnet ein Dialogfeld, in dem Sie eine Scan- und Reparatureinstellung auswählen können; anschließend können Sie durch Klicken auf **OK** einen sofortigen Security-Scan auf dem Gerät ausführen.
- **Antivirus – Jetzt scannen:** Öffnet ein Dialogfeld, in dem Sie Antivirus-Einstellungen auswählen können. Klicken Sie anschließend auf **OK**, um einen sofortigen Antivirus-Scan auf dem Gerät ausführen.
- **Lokale Benutzer und Gruppen verwalten:** Öffnet das Dialogfeld "Lokale Benutzer und Gruppen verwalten". Von diesem Dialogfeld aus können Sie die lokalen Benutzer und Gruppen eines Windows-Geräts remote verwalten.
- **Ausschneiden:** Entfernt Elemente aus einer benutzerdefinierten Gruppe. Sie können keine Elemente aus den Gruppen "Alle" ausschneiden.
- **Kopieren:** Erstellt eine Kopie des Elements, das Sie zu einer anderen Gruppe hinzufügen können.
- **Einfügen:** Fügt das ausgeschnittene oder kopierte Element in eine benutzerdefinierte Gruppe ein.
- **Entfernen:** Entfernt das Element aus einer benutzerdefinierten Gruppe.
- **Löschen:** Löscht das Element aus der Gruppe "Alle" und aus allen anderen Gruppen, denen es gegenwärtig angehört.
- **Eigenschaften:** Zeigt die Inventarzusammenfassung des Geräts sowie Geräteinformationen, Agentenstatus und Remotesteuerungseinstellungen an.

Dieses Hilfethema deckt nicht alle Aspekte des möglichen Kontextmenüs eines jeden Objekts ab. Klicken Sie der rechten Maustaste auf ein beliebiges Element, um die verfügbaren Optionen einzublenden.

HINWEIS: Ihre Firewall blockiert UDP-Pakete
Wenn Sie Geräte über eine Firewall verwalten, die UDP-Pakete blockiert, können Sie die folgenden Funktionen im Kontextmenü dieser Geräte nicht verwenden: **Reaktivieren**, **Herunterfahren**, **Neustart** und **Inventarscan**.

Statusleiste

In der Statusleiste auf der Unterseite der Konsole wird Folgendes angezeigt (von links nach rechts):

Elemente der Statusleiste

- Anzahl der ausgewählten Elemente in einer Liste
- Aktueller Auftragsname und -status
- Name des gegenwärtig angemeldeten Benutzers

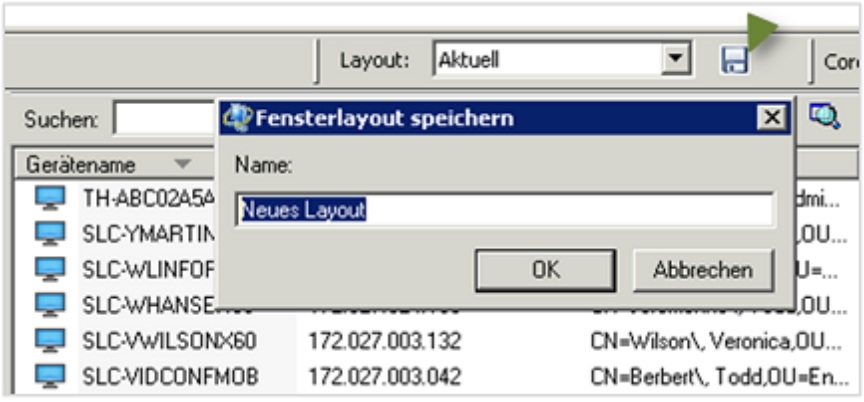
Speichern von Konsolenlayouts

Layouts sind gespeicherte Konsolenkonfigurationen, einschließlich der Position und der Größe des Fensters "Netzwerkansicht", der Toolbox und aller geöffneten Extra-Fenster. Sie können Fensterlayouts verwenden, um benutzerdefinierte Konsolenkonfigurationen zu speichern und wiederherzustellen, die besonders hilfreich für bestimmte Benutzertasks sind.

Um das Layout der Konsole zu ändern, wählen Sie ein gespeichertes Layout aus der Liste **Layout** in der Hauptsymbolleiste aus.

So speichern Sie das gegenwärtige Layout

1. Konfigurieren Sie die Benutzeroberfläche der Konsole Ihren Vorstellungen entsprechend.
2. Klicken Sie in der Symbolleiste neben der Liste **Layout** auf die Schaltfläche **Festplatte**.
3. Geben Sie einen eindeutigen Namen für das Layout ein.
4. Klicken Sie auf **OK**.



Informationen zum Dialogfeld "Fensterlayouts verwalten"

Verwenden Sie dieses Dialogfeld zum Verwalten von gespeicherten Fensterlayouts und zum Zurücksetzen des Konsolenfensters auf das vorherige Layout.

- **Gespeicherte Layouts:** Führt alle von Ihnen gespeicherten Layouts auf.
- **Zurücksetzen:** Stellt das vorherige Layout des Konsolenfensters wieder her.
- **Löschen:** Entfernt das ausgewählte Layout.
- **Umbenennen:** Damit können Sie den Namen des ausgewählten Layouts ändern.

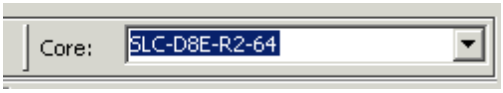
Ändern der Coreserver-Verbindung

Mit der Konsole können Sie den Inhalt einer jeden Datenbank anzeigen und verwalten, die mit einem Coreserver assoziiert ist, mit dem Sie eine Verbindung im Netzwerk herstellen können. Auf diese Weise können Sie Datenbanken für verschiedene Standorte, Organisationseinheiten oder logische interne Netzwerke erstellen.

Sie können immer nur mit jeweils einem Coreserver verbunden sein.

So ändern Sie Coreserver-Verbindungen

1. Wählen Sie einen Coreserver aus der Liste **Core** rechts neben der Symbolleiste der Konsole aus. Sie können auch den Namen eines Coreservers in das Textfeld **Core** eingeben und die **Eingabetaste** drücken.

   Ihr Netzwerk wird nach dem Server durchsucht. Wenn er gefunden wurde, werden Sie aufgefordert, sich beim Standarddialogfeld für die Anmeldung anzumelden.

2. Geben Sie Ihren Benutzernamen und das Kennwort ein.

Halten Sie die üblichen Windows-Richtlinien für die Remoteanmeldung ein (d. h., wenn der Benutzer ein lokaler Benutzer dieses Coreservers ist, geben Sie lediglich den Benutzernamen ein; wenn es sich hingegen um einen Domänenbenutzer handelt, geben Sie den Domänennamen\Benutzernamen ein).

Sobald Sie mit dem Coreserver verbunden sind, wird dessen Name automatisch zur Liste **Core** in der Symbolleiste hinzugefügt.

Sie können sich auch schnell als ein anderer Benutzer beim aktuellen Core anmelden, indem Sie auf die Liste **Core** klicken und die **Eingabetaste** drücken, ohne den Corenamen zu ändern.

Anzeigen von Daten mit dem Inspector

Der LANDesk Management Suite Inspector zeigt Einzelheiten zu Elementen in der LANDesk Konsole an. Mit dem Inspector können Sie innerhalb kürzester Zeit Informationen zu verwalteten Geräten, Abfragen, Sicherheitskonfigurationen und vielen anderen Elementen finden.

Für viele Standardelemente ist ein Inspector definiert. So können Sie beispielsweise verwaltete Geräte, geplante Tasks, Anfälligkeiten und den Coreserver mit Hilfe eines Inspectors überprüfen.

Zum Anzeigen des Inspector erforderliche Benutzerrechte

Um den Inspector anzeigen zu können, muss dem Benutzer das entsprechende Recht in der rollenbasierten Administration zugewiesen worden sein. Das Recht "Inspector" besitzt nur eine Option, die für einen Benutzer aktiviert werden kann, die Option "Anzeigen". Wenn ein Benutzer nicht über dieses Recht verfügt, sind "Auto Inspector" und die Kontextmenüoption für den Inspector nicht sichtbar.

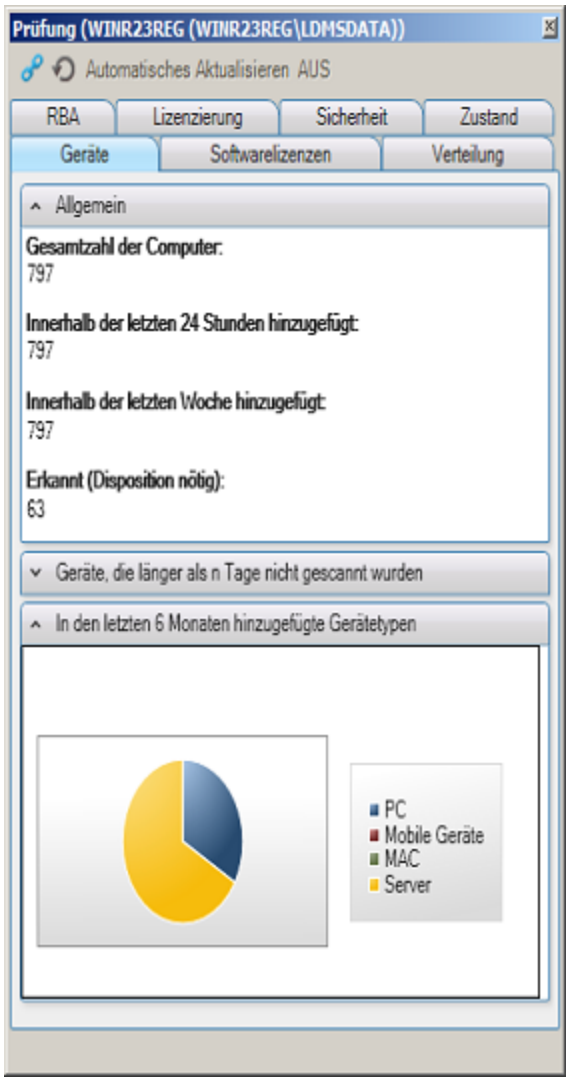
Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Öffnen eines Inspector-Fensters

Daten können auf zweierlei Weise in einem Inspector-Fenster angezeigt werden:

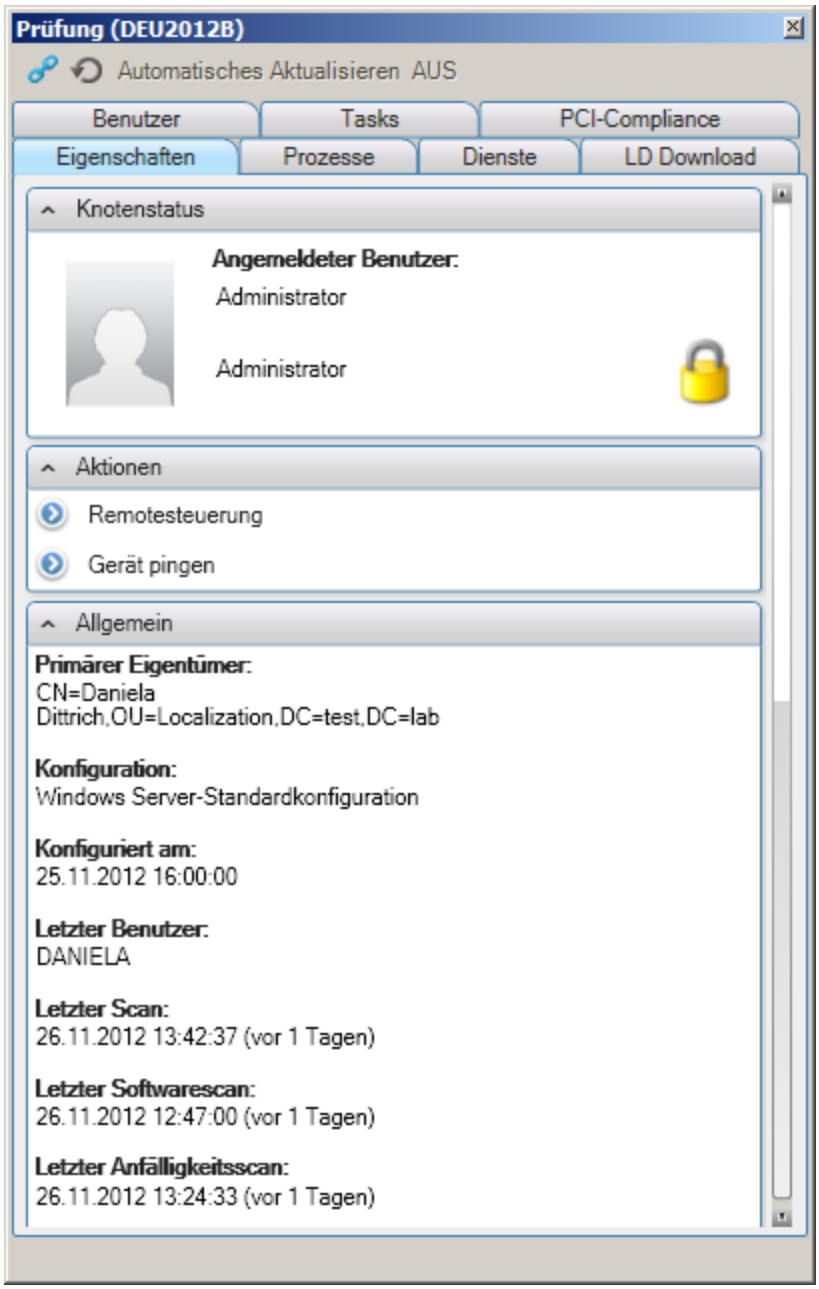
- Schalten Sie den Auto Inspector ein (klicken Sie auf **Ansicht > Auto Inspector**). Damit wird ein Fenster geöffnet, in dem immer dann Daten angezeigt werden, wenn Sie auf ein Element klicken. Jedes Mal, wenn Sie auf ein anderes Element klicken, werden die Daten dieses Elements im Fenster **Auto Inspector** angezeigt.
- Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie **Prüfen** aus. Ein neues Inspector-Fenster mit Daten zu diesem Element wird geöffnet.

Inspector-Fenster werden getrennt von der Konsole geöffnet.

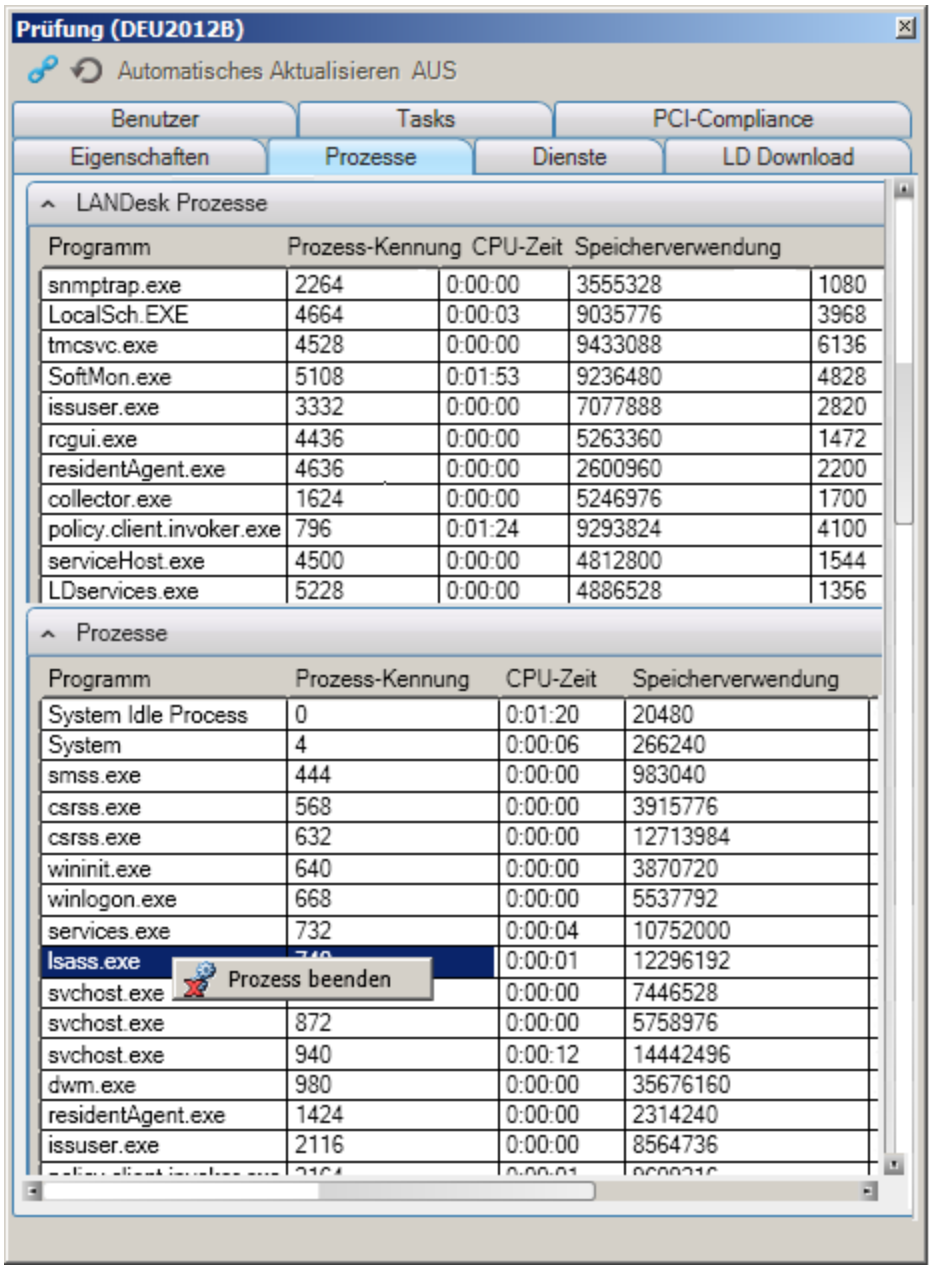


Anzeigen von Inspector-Daten

Inspector-Fenster bieten unterschiedliche Registerkarten und Daten. Elemente werden auf der Basis der für dieses Element definierten XML-Datei angezeigt. Beispielsweise gibt es einen Standard-Inspector für verwaltete Geräte. Wenn Sie auf ein verwaltetes Gerät klicken, sehen Sie im Inspector-Fenster die folgenden Registerkarten:



Sie können die Größe des Fensters zur Anzeige der Daten anpassen. Sie können Aktionen für bestimmte Elemente ausführen, z. B. für die Liste der Prozesse auf einem verwalteten Gerät. Im Inspector-Fenster können Sie auf die Registerkarte **Prozesse** klicken, einen Prozess in der Liste mit Rechtsklick markieren und ihn abbrechen.

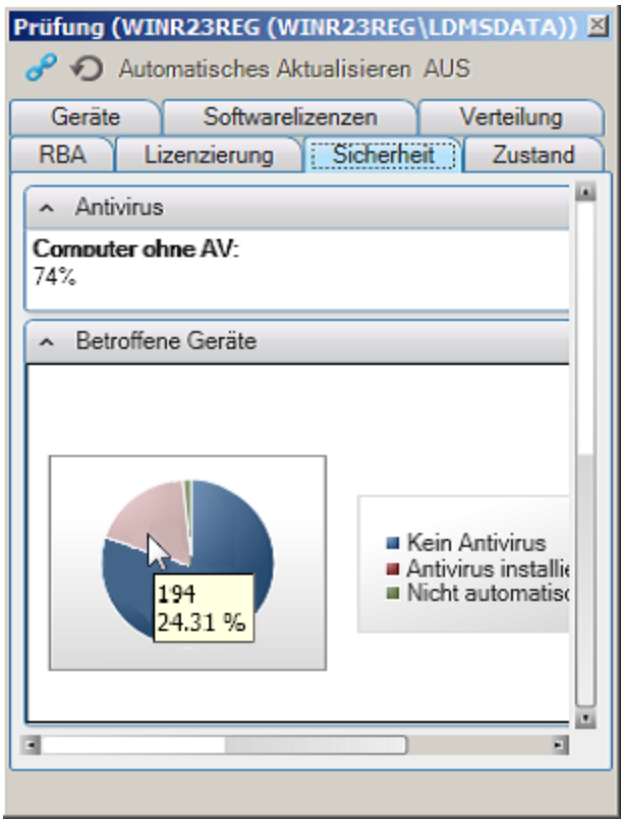


Ähnlich können Sie auch die auf einem Gerät ausgeführten Diensten stoppen oder starten, indem Sie auf die Registerkarte **Dienste** klicken und mit der rechten Maustaste auf einen Dienst in der Liste klicken.

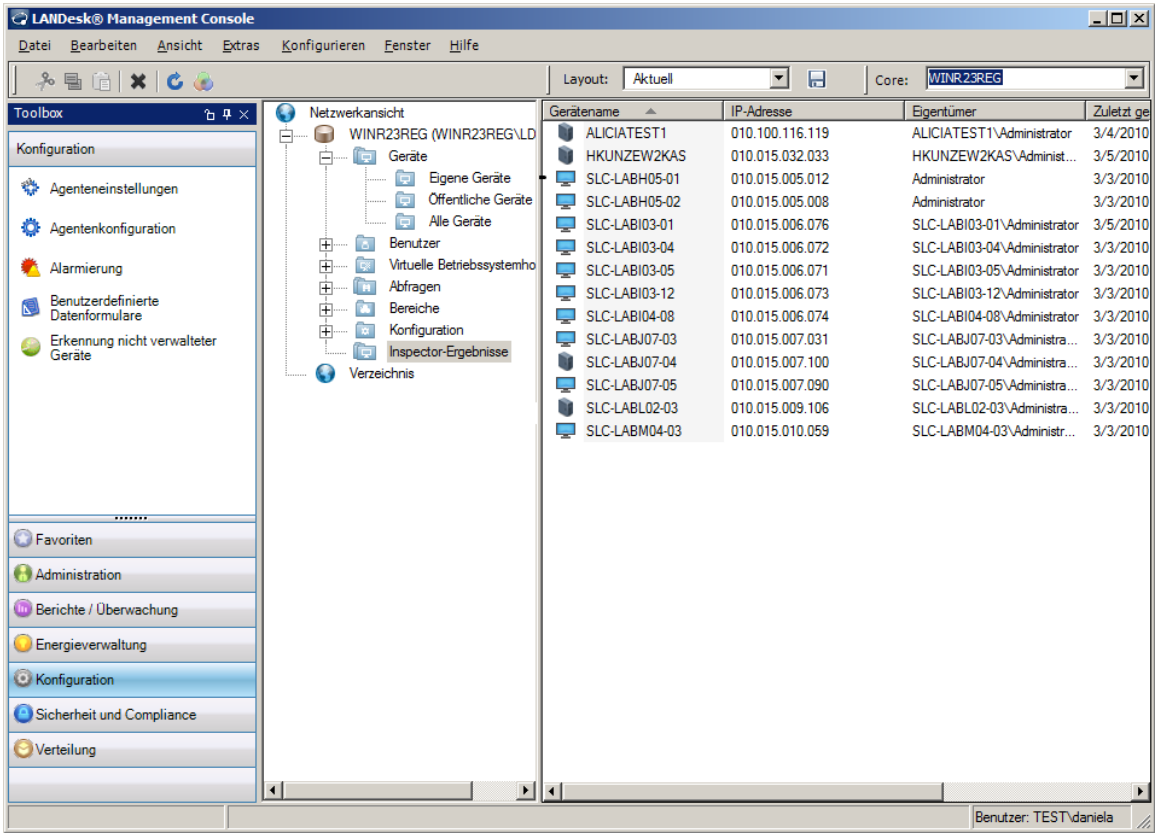
Anzeigen von Inspector-Ergebnissen

Manche Datenelemente in einem Inspector-Fenster werden in Form von Diagrammen angezeigt. Um die Details eines Diagramms anzuzeigen, doppelklicken Sie auf das Diagramm. Die Datendetails werden in der Netzwerkansicht in der Liste **Inspector-Ergebnisse** angezeigt.

Jedes Diagramm zeigt eine Übersicht der zugehörigen Daten, wenn Sie auf einen Teilbereich des Diagramms zeigen.



Doppelklicken Sie auf das Diagramm, um die zugehörigen Daten im Listenformat anzuzeigen.



Werden die Ergebnisse auf diese Weise angezeigt, können Aktionen für die Daten ausgeführt werden. Im Inspector "Geplante Tasks" gibt beispielsweise ein Diagramm, das anzeigt, bei wie vielen Geräten ein Task fehlgeschlagen ist. Wenn Sie auf das Diagramm doppelklicken, sehen Sie die einzelnen Geräte im Order **Inspector-Ergebnisse** aufgelistet. Sie können dann eine Aktion auf diese Geräte anwenden (z. B. den Task neu starten) oder einen Bericht mit den entsprechende Daten anzeigen, sodass Sie nachfassen können.

Die Daten im Order **Inspector-Ergebnisse** ändern sich jedes Mal, wenn Sie in einem Inspector-Fenster auf ein Diagramm klicken. Im obigen Beispiel würden Sie im Diagramm auf den Teilbereich "Kein Antivirus" klicken, um eine Liste der Geräte anzuzeigen, auf denen keine Antivirusanwendung installiert ist. Wenn Sie im Diagramm auf den Bereich "Antivirus installiert" klicken, ändert sich der Inhalt der Liste und es werden Geräte angezeigt, auf denen eine Antivirusanwendung installiert ist.

Echtzeitdaten in Inspector-Anzeigen

Manchen Inspector-Daten können in Echtzeit aktualisiert werden. Dies ist jedoch nur möglich, wenn Sie einen Geräteagenten bereitgestellt haben, der die Komponente "Echtzeitinventar und Überwachung" umfasst.

So überprüfen Sie, ob auf einem Gerät ein Agent für Echtzeitinventar und Überwachung vorhanden ist

1. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf das Gerät und wählen Sie **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Agenten**.

Standard-Inspectors

Die folgenden vordefinierten Inspectors werden bei der Installation der Add-ons "Inspector" installiert

- Spaltensätze
- Computerabfragen
- Konsolenbenutzer
- Konsolenbenutzergruppen
- Coreserver
- Verteilungsmethoden
- Verteilungspakete
- Abfragen
- Rollen
- Geplante Tasks
- Bereiche
- Skripte
- Teams
- Anfälligkeiten

Erstellen von benutzerdefinierten Inspectors

Sie können eine XML-Datei erstellen, die Inspector-Parameter für Elemente in der LANDesk Management Console definiert. Hierzu müssen Sie mit den XML-Konventionen vertraut sein und Sie müssen verstehen, wie Daten in der von Ihrem Coreserver verwendeten Datenbank verwaltet werden.

Anweisungen zur Erstellung eines benutzerdefinierten Inspectors finden Sie in der LANDesk Community im Dokument "Creating a custom inspector".

HINWEIS: Hilfe zum Inspector auf der Website der LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet technische Dokumente und Benutzerforen zum Inspector. Zugang zur Benutzercommunity erhalten Sie hier: http://community.landesk.com

Automatisches Prüfen von Elementen mit Auto Inspector

Die Funktion "Auto Inspector" verwenden Sie, um detaillierte Informationen zu einem beliebigen Element anzuzeigen, auf das Sie klicken. Jedes Mal, wenn Sie auf ein anderes Element klicken, ändert sich der Inhalt des Inspector-Fensters und zeigt das neue Element an.

1. Klicken Sie auf **Ansicht > Auto Inspector**.
2. Klicken Sie auf ein Element in einer Liste, beispielsweise auf ein verwaltetes Gerät, einen geplanten Task oder eine Anfälligkeit.

Link eines Auto-Inspector-Fensters aufheben

Wenn Sie die Daten in einem Auto-Inspector-Fenster behalten möchten, heben Sie den Link zum Inspector auf.

1. Klicken Sie auf die Schaltfläche **Link aufheben** .

Dies sorgt dafür, dass die in einem Inspector-Fenster aktuell angezeigten Daten erhalten bleiben. Sie können nun auf weitere Elemente klicken, die dann in einem neuen Inspector-Fenster geöffnet werden.

Wenn Sie beispielsweise mehrere Elemente miteinander vergleichen möchten, können Sie den Link für die betreffenden Daten aufheben. Sie heben zunächst den Link des ersten Datenfensters auf und klicken anschließend auf ein neues Element, um ein zweites Inspector-Fenster zu öffnen.

Manuelles Prüfen von Elementen

Wenn Sie die Funktion "Auto Inspector" nicht verwenden, können Sie jedes Element per Rechtsklick prüfen. Jedes Mal, wenn Sie ein Element manuell prüfen, wird ein neues Inspector-Fenster mit den neuen Daten geöffnet.

1. Klicken Sie mit der rechten Maustaste auf ein Listenelement (beispielsweise ein verwaltetes Gerät).
2. Wählen Sie **Prüfen** aus.

Link zu dynamischem Inhalt aufheben

Die Daten im Inspector-Fenster können dynamische Daten sein. Manche Datenelemente werden in regelmäßigen Abständen aktualisiert (wenn ein Gerät eine Echtzeitinventar-Komponente besitzt).

So behalten Sie die in einem Inspector aktuell angezeigten Daten bei

1. Klicken Sie auf die Schaltfläche **Link aufheben** .

Aktualisieren der Daten in einem Fenster, für das der Link aufgehoben wurde

Nachdem Sie den Link für ein Inspector-Fenster aufgehoben haben, können Sie diesen Link für die Daten nicht wiederherstellen, um diese Daten wieder in dynamische Daten zu verwandeln. Die Daten in dem Fenster bleiben unverändert, es sei denn, Sie ändern die Einstellung für die Aktualisierung.

So aktualisieren Sie die Daten in einem Inspector

1. Klicken Sie auf die Schaltfläche **Aktualisierungsrate ändern**

.
2. Der Text neben der Schaltfläche zeigt die aktuelle Einstellung für die Aktualisierung an. Klicken Sie erneut auf die Schaltfläche, um die Einstellung zu ändern. Sie können zwischen 10 Sekunden, 30 Sekunden oder 10 Minuten wählen.

Benutzerverwaltung

Rollenbasierte Administration - Übersicht

LANDesk Management Suite bietet einen sehr umfangreichen Satz rollenbasierter Verwaltungsfunktionen für die Verwaltung von Konsolenbenutzern. Sie haben folgenden Möglichkeiten:

- Zuweisung präziser funktionsbasierter Gruppenberechtigungen
- Frühzeitige Zuweisung von Berechtigungen zu mehreren Benutzer durch lokale oder LDAP-Benutzergruppen
- Synchronisierung von Konsolenbenutzerkonfigurationen über mehrere Coreserver hinweg.

Die von Ihnen erstellten Rollen können auf den Verantwortungsbereichen der Benutzer basieren, den Verwaltungstasks, die Sie den Benutzern einräumen möchten, und den Geräten, auf die die Benutzer zugreifen und die sie verwalten sollen. Der Gerätezugriff lässt sich auf einen Standort, beispielsweise ein Land, eine Region, ein Bundesland, eine Stadt oder sogar ein bestimmtes Büro oder eine Abteilung beschränken. Der Zugriff kann auch auf eine bestimmte Geräteplattform, einen Prozessortyp oder andere Hard- und Softwareattribute der Geräte eingeschränkt werden. Bei der rollenbasierten Administration können Sie frei entscheiden, wie viele Rollen Sie erstellen möchten, welche Benutzer diese Rollen wahrnehmen können und wie groß oder klein ihr Bereich des Gerätezugriffs sein soll. Sie können z. B. einem oder mehreren Benutzer die Rolle des Managers für die Softwareverteilung zuordnen, einen anderen Benutzer für die Remotesteuerungsvorgänge verantwortlich machen, einen weiteren Benutzer mit der Berichterstellung beauftragen usw.

Wenn Sie nicht allzu viele Konsolenbenutzer haben oder den Konsolenbenutzern, die Sie haben, keine Beschränkungen auferlegen wollen, können Sie die rollenbasierte Administration vollständig umgehen und Benutzer einfach zur lokalen Gruppe der LANDesk Administratoren des Coreservers hinzufügen. Die Mitglieder dieser Gruppe haben uneingeschränkten Zugriff auf die Konsole und können alle Geräte verwalten. Standardmäßig wird das Benutzerkonto, mit dem Management Suite installiert wurde, zur Gruppe der LANDesk Administratoren hinzugefügt.

Die rollenbasierte Administration besitzt die Flexibilität, Sie so viele benutzerdefinierte Rollen erstellen zu lassen, wie Sie möchten. Sie können dieselben Berechtigung auch verschiedenen Benutzern zuweisen, den Zugriff dieser Benutzer jedoch auf eine begrenzte Gruppe von Geräten (reduzierter Bereich) limitieren. Sogar ein Administrator kann durch einen Bereich eingeschränkt werden, indem seine Administratoraufgaben auf eine bestimmte geographische Region oder einen bestimmten Typ von verwalteten Geräten eingeschränkt wird. Wie Sie am besten von der rollenbasierten Administration profitieren, hängt von Ihren Netzwerk- und Personalressourcen und Ihrem individuellen Unternehmensbedarf ab.

HINWEIS: Wenn Sie ein Upgrade von Management Suite 8 vorgenommen haben, erstellt das Setupprogramm im Verzeichnis ...\LANDesk\Management Suite eine Protokolldatei mit dem Namen RBAUpgradeReport.txt. Diese Datei enthält Informationen, die Ihnen bei der Zuordnung von 8.x-Rollen zu 9.x helfen.

Weitere Informationen zur Verwendung von Rollen finden Sie in den folgenden Abschnitten:

- "Hinzufügen von Management Suite Konsolenbenutzern" auf Seite 41
- "Verwalten von Authentifizierungen" auf Seite 44
- "Verwalten von Rollen" auf Seite 46
- "Erläuterungen zu Rechten und Status" auf Seite 48

- "Erstellen von Bereichen" auf Seite 57
- "Verwenden von Teams" auf Seite 60

Rollenbasierte Administration – Prozessablauf

Nachstehend sind die wesentlichen Prozessschritte für den Einsatz der rollenbasierten Administration beschrieben:

1. Erstellen von Rollen für Konsolenbenutzer.
2. Hinzufügen von Konsolenbenutzern zu den entsprechenden Windows LANDesk Gruppen mithilfe des Windows-Extras "Lokale Benutzer und Gruppen".
3. Erstellen von Authentifizierungen für jedes Active Directory, das Sie für die Bestimmung von Konsolenbenutzern verwenden werden.
4. Verwendung von Bereichen, um die Liste der Geräte zu beschränken, die von Konsolenbenutzern verwaltet werden können (optional).
5. Verwendung von Teams zur weiteren Kategorisierung von Konsolenbenutzern.

Hinzufügen von Management Suite Konsolenbenutzern

Management Suite-Benutzer können sich an der Konsole anmelden und bestimmte Aufgaben für bestimmte Geräte im Netzwerk durchführen. Der Benutzer, der während der Installation von Management Suite am Server angemeldet ist, wird automatisch zu einem Mitglied der Benutzergruppe "Windows **LANDesk Administratoren**" gemacht und damit mit vollen Administratorrechten ausgestattet. Dieser Benutzer ist für das Hinzufügen weiterer Benutzergruppen zur Konsole und für die Zuweisung von Berechtigungen und Bereichen zuständig. Nachdem weitere Administratoren erstellt wurden, können diese dieselben administrativen Aufgaben durchführen.

Management Suite Setup erstellt mehrere lokale Windows-Gruppen auf dem Coreserver. Diese Gruppen steuern die Dateisystemberechtigungen für die Management Suite Programmordner auf dem Coreserver. Konsolenbenutzer müssen folgenden lokalen Windows-Gruppen manuell hinzugefügt werden:

- **LANDesk Management Suite:** Diese Gruppe gewährt einfachen Zugriff auf den Core. Die Management Suite Ordner sind schreibgeschützt. Benutzer in dieser Gruppe können nicht in das Skriptverzeichnis schreiben und daher keine Skripte verwalten. Die Reparatur von Anfälligkeiten und die Betriebssystembereitstellung funktionieren für Benutzer in dieser Gruppe nicht korrekt, da beide Funktionen Skripte verwenden.
- **LANDesk Script Writers:** Diese Gruppe ermöglicht es Benutzern, in den Ordner der Skripte zu schreiben. Das Patchen von Anfälligkeiten und die Betriebssystembereitstellung setzen eine Mitgliedschaft in dieser Gruppe voraus. Diese Gruppe gewährt keine anderen administrativen Privilegien.
- **LANDesk Administratoren:** Dies ist die ausfallsichere Gruppe für den Konsolenzugriff. Jedes Mitglied dieser Gruppe hat vollständige Rechte in der Konsole, einschließlich des Schreibrechts für Skripte. Standardmäßig wird das Benutzerkonto, mit dem Management Suite installiert wurde, zu dieser Gruppe hinzugefügt. Wenn Sie nicht allzu viele Konsolenbenutzer haben oder den Konsolenbenutzern, die Sie haben, keine Beschränkungen auferlegen wollen, können Sie die rollenbasierte Administration vollständig umgehen und Benutzer einfach zu dieser Gruppe hinzufügen.

Beim Hinzufügen von Administratoren mit vollständigen Rechte zur Konsole können Sie diese entweder zur Gruppe der lokalen LANDesk Administratoren hinzufügen oder Sie können Sie zu einer anderen Gruppe hinzufügen, die über das LANDesk "Administrator"-Recht verfügt. Der einzige Unterschied besteht darin, dass Benutzer in der Windows-Gruppe "LANDesk Administratoren" erst dann von der Konsole gelöscht werden können, wenn Sie zuvor aus der Gruppe "LANDesk Administratoren" entfernt wurden.

Die Stukturansicht **Benutzer und Gruppen** des Extras "Benutzer" zeigt die Liste der autorisierten Konsolenbenutzer an. Sie können sehen, wann sich ein Konsolenbenutzer das letzte Mal angemeldet hat, welcher Gruppe er angehört, welche Rolle und welcher Bereich ihn zugeordnet ist, welche Zeitbeschränkung für die Remotesteuerung definiert ist und welchem Team er angehört. Sie können diese Strukturansicht auch verwenden, um herauszufinden, ob Benutzer den lokalen LANDesk Windows-Gruppen angehören. Benutzer können sich erst anmelden, wenn Sie diese zu einer der in diesem Abschnitt beschriebenen LANDesk Gruppen hinzugefügt haben.

Benutzer werden in der Datenbank unter Verwendung eindeutiger Kennungen (SIDs) gespeichert. Wenn sich der Name des Active Directory-Kontos eines Benutzers ändert, beispielsweise aufgrund einer Heirat, sollte seine SID unverändert bleiben und die Management Suite-Berechtigungen bleiben gültig.

WICHTIG: Zusätzliche Konsolen und der Coreserver müssen Mitglieder derselben Domäne oder Arbeitsgruppe sein. Konsolenbenutzer können sich nicht bei einem Coreserver authentifizieren, der sich in einer anderen Domäne oder Arbeitsgruppe befindet.

Hinzufügen von Management Suite Konsolenbenutzern

Management Suite-Benutzer können sich an der Konsole anmelden und bestimmte Aufgaben für bestimmte Geräte im Netzwerk durchführen. Der Benutzer, der während der Installation von Management Suite am Server angemeldet ist, wird automatisch zu einem Mitglied der Benutzergruppe "Windows **LANDesk Administratoren**" gemacht und damit mit vollen Administratorrechten ausgestattet. Dieser Benutzer ist für das Hinzufügen weiterer Benutzergruppen zur Konsole und für die Zuweisung von Berechtigungen und Bereichen zuständig. Nachdem weitere Administratoren erstellt wurden, können diese dieselben administrativen Aufgaben durchführen.

So fügen Sie vom Dialogfeld "Windows Computer Management" aus einen Benutzer zu einer LANDesk Gruppe hinzu

1. Navigieren Sie zum Dienstprogramm **Verwaltung > Computerverwaltung > Lokale Benutzer und Gruppen > Gruppen** des Servers.
2. Klicken Sie mit der rechten Maustaste auf die gewünschte LANDesk Gruppe und wählen Sie dann **Zur Gruppe hinzufügen** aus.
3. Klicken Sie im Dialogfeld **Eigenschaften** der Gruppe auf **Hinzufügen**.
4. Wählen Sie im Dialogfeld **Wählen Sie die Benutzer und Gruppen aus** die gewünschten Benutzer (und Gruppen) in der Liste aus und klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **OK**.

So fügen Sie einen Management Suite-Konsolenbenutzer oder eine Management Suite-Gruppe hinzu:

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie in der Strukturansicht **Benutzer und Gruppen** mit der rechten Maustaste auf die Authentifizierungsquelle, die den gewünschten Benutzer bzw. die gewünschte Gruppe enthält und klicken Sie dann auf **Neuer Benutzer oder neue Gruppe**.
3. Wählen Sie im Quellverzeichnis für die Authentifizierung den Benutzer oder die Gruppe aus, den bzw. die Sie hinzufügen möchten und klicken Sie auf **Hinzufügen**. Wenn Sie einzelne Benutzer innerhalb einer Gruppe auswählen möchten, klicken Sie mit der rechten Maustaste zunächst auf die Gruppe und klicken Sie dann auf **Wählen Sie die Benutzer aus, die hinzugefügt werden sollen**. Anschließend können Sie die gewünschten Benutzer auswählen und auf **Ausgewählte Benutzer hinzufügen** klicken.
4. Klicken Sie in dem Dialogfeld mit der Erinnerung, den von Ihnen ausgewählten Benutzer bzw. die Gruppe manuell zur entsprechenden lokalen LANDesk Windows-Gruppe hinzuzufügen, auf **OK**.
5. Klicken Sie auf **Schließen**.
6. Wenn nicht bereits geschehen, verwenden Sie das Windows-Extra **Lokale Benutzer und Gruppen**, um den neuen Benutzer bzw. die neue Gruppe wie zuvor in diesem Abschnitt beschrieben zur entsprechenden lokalen LANDesk Windows-Gruppe hinzuzufügen.
7. Weisen Sie dem neuen Benutzer bzw. der neuen Gruppe Rollen und Bereiche zu.

Löschen von Benutzern

Sie können die Strukturansicht **Benutzer und Gruppen** auch zum Löschen von Benutzern oder Gruppen verwenden. Wenn Sie einen Benutzer oder eine Gruppe löschen, werden Sie aufgefordert, zu entscheiden, wie mit den Konsolenelementen verfahren werden soll, deren Eigentümer der Benutzer bzw. die Gruppe ist, wie beispielsweise Abfragen, geplante Tasks und so weiter. Sie können die Konsole anweisen, automatisch alle Elemente zu löschen, die diesen gehören. Sie können die Konsole aber auch anweisen, diese Elemente einem anderen Benutzer oder einer anderen Gruppe zuzuordnen, den bzw. die Sie bestimmen. Beachten Sie, dass die Löschung eines Benutzers oder einer Gruppe lediglich den Benutzer- oder Gruppeneintrag in der Management Suite Benutzerdatenbank löscht. Sie müssen den Benutzer bzw. die Gruppe außerdem manuell aus allen lokalen LANDesk Windows-Gruppen löschen, bei denen er bzw. sie Mitglied ist. Wenn Sie dies nicht tun, kann sich der gelöschte Benutzer immer noch in der Konsole anmelden.

So löschen Sie einen Konsolenbenutzer

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie in der Struktur **Benutzerverwaltung** auf **Benutzer und Gruppen**.
3. Wählen Sie den Benutzer oder die Gruppe aus, den bzw. die Sie löschen möchten, und drücken Sie die Taste ENTF.
4. Wenn Sie mit dem Benutzer verknüpfte Objekte löschen möchten, klicken Sie auf **OK**.
5. Wenn Sie eine Neuzuweisung der mit dem Konsolenbenutzer verknüpften Objekte vornehmen wollen, wählen Sie **Folgendem Benutzer, folgender Gruppe bzw. folgendem Team Objekte zuweisen:** aus und klicken auf den Benutzer, die Gruppe oder das Team, der/die/das die Objekte erhalten soll, und klicken Sie auf **OK**.
6. Entfernen Sie den Benutzer aus der lokalen LANDesk Windows-Gruppe oder Active Directory-Gruppe, die ihm Konsolenzugriff gewährt.

Anzeigen der Benutzer- oder Gruppeneigenschaften

In der Strukturansicht **Benutzer und Gruppen** können Sie mit der rechten Maustaste auf den Benutzer oder die Gruppe im rechten Ausschnitt klicken und dann **Eigenschaften** auswählen. Das Dialogfeld "Eigenschaften" zeigt alle Eigenschaften und effektiven Rechte für den betreffenden Benutzer an. Das Dialogfeld "Eigenschaften" umfasst die folgenden Seiten:

- **Übersicht:** Ein Zusammenfassung der Rollen, Bereiche, Teams, Gruppenmitgliedschaften und effektiven Rechte des betreffenden Benutzers bzw. der betreffenden Gruppe.
- **Effektive Rechte:** Eine detailliertere Ansicht der effektiven Rechte des Benutzers bzw. der Gruppe.
- **Rollen:** Zeigt explizite und vererbte Rollen. Sie können wählen, welche expliziten Rollen für diesen Benutzer oder für diese Gruppe gelten.
- **Bereiche:** Zeigt explizite und vererbte Bereiche. Sie können wählen, welche expliziten Bereiche für diesen Benutzer oder für diese Gruppe gelten.
- **Teams:** Zeigt explizite und vererbte Teams. Sie können wählen, welche expliziten Teams für diesen Benutzer oder für diese Gruppe gelten.
- **RC-Zeitbeschränkungen:** Dient der Übernahme und Änderung von RC-Zeitbeschränkungen. Weitere Informationen finden Sie unter "Verwenden der Zeitbeschränkungen für die Remotesteuerung" auf Seite 61.
- **Gruppenmitgliedschaft:** Zeigt die Gruppen an, denen der Benutzer angehört.
- **Gruppenmitglieder:** Zeigt die Mitglieder einer Gruppe an, wenn eine Gruppe ausgewählt wurde. Zeigt die Gruppe an, der ein Benutzer angehört, wenn ein Benutzer ausgewählt wurde.

Wenn Sie Änderungen an bearbeitbaren Seiten vornehmen, müssen Sie auf OK klicken, damit Ihre Änderungen übernommen werden. Sie können das Dialogfeld "Eigenschaften", falls erforderlich, erneut aufrufen.

Verwalten von Authentifizierungen

Das Extra "Benutzerverwaltung" verwenden Sie zur Definition der Anmeldeinformationen für Active Directory-Gruppen, die Zugriff auf die Konsole haben werden. Diese Anmeldeinformation müssen lediglich dafür sorgen, dass Management Suite das Verzeichnis auflistet. Sie müssen Anmeldeinformationen für jedes Active Directory bereitstellen, das Benutzer enthält, die Konsolenzugriff haben sollen. Die von Ihnen bereitgestellten Authentifizierungen bestimmen, welche Benutzergruppen Sie bei der Zuweisung von Konsolengruppenberechtigungen auswählen können.

Die Konsolenauthentifizierung basiert auf der Mitgliedschaft in einer lokalen Windows-Gruppe oder einer Active Directory-Gruppe. Wenn ein LANDesk Administrator einer lokalen oder Active Directory-Gruppe Gruppenberechtigungen zuweist, können sich Benutzer, die Mitglieder der betreffenden Gruppe sind, bei der Windows- oder Webkonsole anmelden und die dieser Gruppe zugewiesen Berechtigungen mit nutzen.

Bei der Verwaltung von Aktive Directories zwecks Verwendung mit Management Suite müssen Sie Folgendes beachten:

- Active Directory ist vollständig in DNS integriert und TCP/IP (DNS) ist erforderlich. Der DNS-Server muss Ressourceneinträge für Dienste (SRV-Einträge) bzw. Dienstaufzeichnungen unterstützen.

- Wenn ein Benutzer mithilfe von Active Directory zu einer in der Konsole verwendeten Gruppe hinzugefügt wird, dann kann sich dieser Benutzer nicht bei der Konsole anmelden, obwohl ihm Management Suite Berechtigungen zugewiesen wurden. Ein Benutzer muss den lokalen LANDesk Gruppen des Coreservers angehören, damit er sich bei der Konsole anmelden kann. Weitere Informationen finden Sie unter "Hinzufügen von Management Suite Konsolenbenutzern" auf Seite 41.
- Damit Aktive Directories ordnungsgemäß mit der rollenbasierten Administration zusammenarbeiten, müssen Sie die COM+-Server-Anmeldeinformationen auf dem Coreserver konfigurieren. Dies ermöglicht es dem Coreserver, ein Konto in einer der lokalen LANDesk Gruppen des Coreservers zu verwenden, das über die erforderlichen Berechtigungen zum Auflisten von Windows-Domänenmitgliedern verfügt, wie beispielsweise das Administratorkonto. Anweisungen zum Durchführen der Konfiguration finden Sie unter "Konfigurieren von COM+-Serveranmeldeinformationen" auf Seite 78.

Wenn sich das Kennwort des Kontos für eine Authentifizierung ändert, müssen Sie sich bei der Konsole anmelden und das Kennwort im Authentifizierungsdialogfeld in das neue Kennwort ändern. Sie tun dies, indem Sie sich als lokale Gruppe anmelden. Benutzer werden bei der Anmeldung authentifiziert, d. h. jede bestehende Sitzung bleibt funktionstüchtig. Benutzer in der Domäne, deren Kennwort geändert wurde, dürfen sich erst anmelden, wenn die Kennwortänderung im Extra "Benutzer" korrigiert wurde.

Einrichten von Rechten mit Active Directory

Beim Einsatz von Active Directory mit RBA (Run Book Automation) gelten die folgenden Regeln:

- Wenn ein Benutzer Mitglied einer Active Directory-Gruppe ist, "erbt" der Benutzer die RBA-Rechte für diese Gruppe.
- Wenn ein Benutzer Mitglied einer Active Directory-Gruppe ist, die Mitglied einer übergeordneten Gruppe ist, "erbt" der Benutzer die RBA-Rechte der Gruppe auf der übergeordneten Ebene.
- Gruppen können geschachtelt werden und erben die entsprechenden Rechte in Übereinstimmung mit den Active Directory-Regeln.

Hinzufügen einer Active Directory-Authentifizierung

Das Extra "Benutzerverwaltung" verwenden Sie zur Definition der Anmeldeinformationen für Active Directory-Gruppen, die Zugriff auf die Konsole haben werden. Diese Anmeldeinformation müssen lediglich dafür sorgen, dass Management Suite das Verzeichnis auflistet. Sie müssen Anmeldeinformationen für jedes Active Directory bereitstellen, das Benutzer enthält, die Konsolenzugriff haben sollen. Die von Ihnen bereitgestellten Authentifizierungen bestimmen, welche Benutzergruppen Sie bei der Zuweisung von Konsolengruppenberechtigungen auswählen können.

So fügen Sie eine Authentifizierung hinzu

1. Klicken Sie im Extra **Benutzerverwaltung** mit der rechten Maustaste auf **Benutzer und Gruppen** und klicken Sie dann auf **Neue Authentifizierungsquelle**.
2. Geben Sie im Dialogfeld **Authentifizierungsquelle** die Anmeldeinformationen ein, die Zugriff auf das Active Directory gewähren.
3. Klicken Sie auf **OK**.

Anpassen der Frequenz von Verzeichnisabfragen

Seit LDMS 9 SP2 gibt es ein Dienstprogramm mit der Bezeichnung Resolveusergroups.exe. Dieses Dienstprogramm wird in regelmäßigen Abständen (all 20 Minuten) ausgeführt, um die Liste der LANDesk Management Suite-Konsolenbenutzer zu aktualisieren.

Sobald die Benutzerliste aufgelöst ist, wird sie in den Cache gestellt und verwendet, bis Resolveusergroups.exe erneut ausgeführt wird. In manchen Active Directory-Umgebungen kann es bei zu kleinen TTL-Werten vorkommen, dass der TTL-Schwellenwert bei manchen der aufgelösten Benutzerkonten unter Umständen bereits überschritten ist, bevor alle anderen Konten aufgelöst sind. Dies führt dazu, dass der Cache wieder und wieder aktualisiert wird und die Konsole sehr langsam lädt.

Falls dieser Fall in Ihrer Umgebung eintreten sollte, ändern Sie die TTL-Standardeinstellungen für Resolveusergroups.exe. Wenn Sie wissen wollen, wie dieses Programm verwendet wird, führen Sie Resolveusergroups.exe /? aus. Die TTL-Werte sind in Sekunden ausgewiesen. Hier ist ein spezifisches Beispiel, bei dem die TTL-Werte auf die Höchstwerte gesetzt werden:

```
Resolveusergroups.exe /verbose /TTL 600 /LDTTL 60
```

Alle für die TTL-Werte vorgenommenen Änderungen werden in die KeyValue-Tabelle in der Datenbank geschrieben (GroupResolutionTTL und LocalLDGroupResolutionTTL), damit sie Bestand haben.

Verwalten von Rollen

Den Rollenbaum verwenden Sie für die Definition und Verwaltung administrativer Rollen und der mit diesen verknüpften Konsolenrechte. Konsolenrechte bauen auf Management Suite Funktionen auf. Sie könnten beispielsweise eine Rolle namens "Help Desk" erstellen und dieser Rolle das Recht zur Remotesteuerung geben.

Sie können beliebig viele zusätzliche Rollen hinzufügen. Neue Rollen werden nicht automatisch Benutzern oder Gruppen zugewiesen. Sobald Sie eine Rolle erstellt haben, ordnen Sie diese im Baum "Gruppenberechtigungen" einem Benutzer oder einer Gruppe zu.

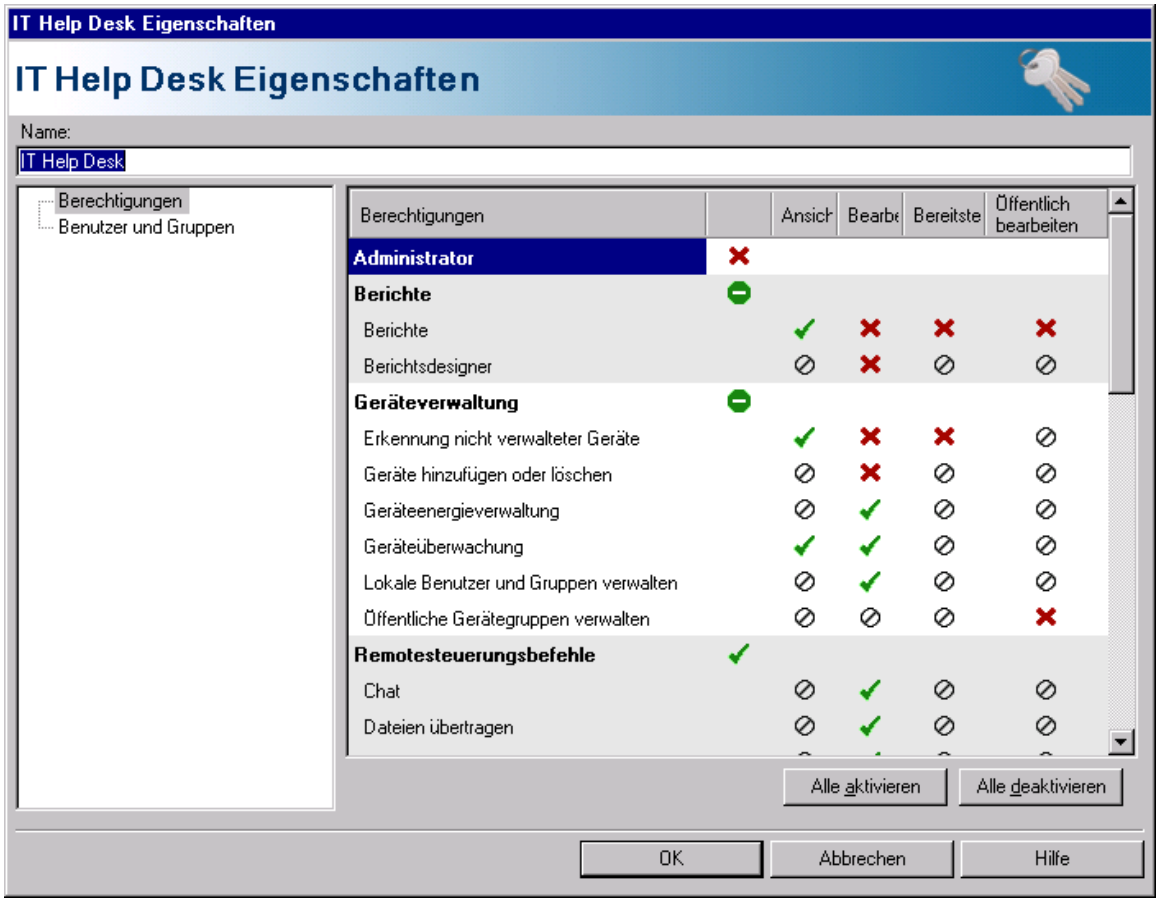
Da Sie Benutzern oder Gruppen mehrere Rollen zuweisen können, müssen Sie entscheiden, wie Sie Rechte zuweisen. Sie können Rechte entweder auf der Basis einer Funktionsbeschreibung wie zum Beispiel "Help Desk" zuweisen oder Sie können Rechte auf der Basis von Konsolenfunktionen zuweisen, wie etwa "Remotesteuerung". Je nach der Anzahl und Zusammensetzung der Konsolenbenutzer in Ihrer Organisation ist einer dieser beiden Ansätze vermutlich besser geeignet als der andere.

Sie können einem einzelnen Benutzer oder einer einzelnen Active Directory-Gruppe mehrere Rollen zuweisen. Wenn es zwischen den ausgewählten Rollen widersprüchliche Rechte gibt, umfasst die Gruppenberechtigung die Summe der kombinierten Rollen und Bereiche. Beispiel: Wenn eine eingeschlossene Rolle Remotesteuerung erlaubt und eine andere eingeschlossene Rolle sie verweigert, dann erlaubt die daraus resultierende Gruppenberechtigung die Remotesteuerung. Sie können die effektiven Rechte eines Benutzers oder einer Gruppe einsehen, indem Sie die zugehörigen Eigenschaften öffnen und die Seite **Effektive Rechte** anzeigen.

Generell sollten Sie es vermeiden, den folgenden lokalen Standardgruppen eine Rolle zuzuweisen: LANDesk Management Suite, LANDesk Script Writers und LANDesk Administratoren. Wird einer Gruppe eine Rolle zugewiesen, so betrifft dies alle Gruppenmitglieder. Da alle Konsolenbenutzer Mitglied einer dieser drei Gruppen sein müssen, könnte es passieren, dass Sie unbeabsichtigterweise für alle den Zugriff auf Konsolenfunktionen einschränken. Die Gruppe "LANDesk Administratoren" verfügt bereits über die Standardrolle "Administrator", die nicht weiter eingeschränkt werden kann.

Änderungen, die Sie für die Rechte eines angemeldeten Benutzers vornehmen, werden erst nach der erneuten Anmeldung dieses Benutzers wirksam.

Nähere Informationen finden Sie unter "Erläuterungen zu Rechten und Status" auf Seite 48 und "Erläuterungen zu den Standardrollen" auf Seite 48.



Erstellen und Zuweisen einer Rolle

Rollen dienen der Definition und Verwaltung von administrativen Rollen und den mit diesen verknüpften Konsolenrechten.

So erstellen Sie eine Rolle und weisen diese zu

1. Klicken Sie im Extra **Benutzerverwaltung** mit der rechten Maustaste auf **Rollen** und klicken Sie dann auf **Neue Rolle**.
2. Geben Sie im Dialogfeld **Rolleneigenschaften** einen Rollen**namen** ein.
3. Aktivieren oder deaktivieren Sie die gewünschten Rechte, indem Sie auf das Symbol in der zugehörigen Spalte klicken. Mit jedem Klick wechselt der Status eines Rechts.
4. Klicken Sie im Baum auf **Benutzer und Gruppen** und wählen Sie die Benutzer und Gruppen aus, denen Sie die neue Rolle zuweisen wollen.

So weisen Sie Benutzern und Gruppen eine vorhandene Rolle zu

1. Klicken Sie im Extra **Benutzerverwaltung** mit der rechten Maustaste auf **Rollen** und klicken Sie dann auf **Eigenschaften**. Sie können auch auf eine Rolle doppelklicken, um ihre Eigenschaften zu bearbeiten.
2. Wählen Sie auf der Seite **Benutzer und Gruppen** die Gruppen aus, denen Sie diese Rolle zuweisen möchten.
3. Klicken Sie auf **OK**.

Erläuterungen zu den Standardrollen

Im Rollenbaum gibt es eine Reihe von Standardrollen. Sie können keine dieser Standardrollen bearbeiten oder löschen – mit Ausnahme der Rolle "LANDesk Administrator".

- Überwachungskonfiguration
- Auditor
- Inspector Viewer
- IT Help Desk
- LANDesk Administrator
- Patchmanagement
- Energieverwaltung
- Versorgung (Provisioning)
- Sicherheit
- Softwareverteilung
- Softwarelizenzierung

WICHTIG: LANDesk Administratoren haben uneingeschränkte Rechte
LANDesk Administratoren haben uneingeschränkte Rechte für sämtliche Bereiche und Rechte. Sie haben ferner vollen Zugriff auf das Extra "Benutzer" und können nach Belieben Änderungen vornehmen. Darüber hinaus können nur Benutzer mit dem Administratorrecht LANDesk Dienste konfigurieren, die auf dem Core ausgeführt werden.

Erläuterungen zu Rechten und Status

Ein Benutzer kann vier verschiedene Arten von Rechten haben:

- **Ansicht:** Gestattet Benutzern den Zugriff auf ein Konsolenextra.
- **Bearbeiten:** Gestattet es Benutzern, Änderungen im zugehörigen Konsolenextra vorzunehmen. Dieses Recht schließt das Recht zur Ansicht mit ein.
- **Bereitstellen:** Gestattet es Benutzern, beliebige geplante Tasks zu erstellen, zu ändern oder zu löschen, die mit dem zugehörigen Konsolenextra verknüpft sind.
- **Öffentlich bearbeiten:** Gestattet es Benutzern, Elemente in einem **Öffentlichen** Ordner eines Konsolenextras zu erstellen, zu modifizieren oder zu löschen.

Nicht alle Rechte bieten Unterstützung für alle Typen. So kann das Recht "Verwaltung öffentlicher Abfragen" beispielsweise nur den Typ "Öffentlich bearbeiten" aufweisen. Es würde keinen Sinn ergeben, hier auch die Typen "Ansicht", "Bearbeiten" oder "Bereitstellen" zu haben.

Jedes Recht kann einen der drei folgenden Status aufweisen:

- Ein Häkchen: ✔
- Ein X: ✖
- Ein Symbol "Nicht zutreffend": ⊘

Wenn Sie auf ein Häkchen oder ein X klicken, wechselt dessen Status.

Wenn Benutzer nicht über Rechte für ein Extra verfügen, können sie das Extra nicht sehen, wenn sie sich auf der Konsole anmelden. Das Extra wird dann weder in der Symbolleiste noch im Menü **Extras** angezeigt.

Das Extra **Geplante Tasks** ist nur für Benutzer sichtbar, die ein Recht zum "Bereitstellen" besitzen, und diesem Fall können Sie nur mit Tasks arbeiten, die mit dem Extra verknüpft sind, für das sie Rechte zum Bereitstellen haben. Alle anderen Tasks sind schreibgeschützt.

Erläuterungen zum Recht "Öffentlich bearbeiten"

Die "Öffentliche" Gruppe eines Extras ist für alle Benutzer sichtbar. Elemente in der öffentlichen Gruppe sind schreibgeschützt, es sei den Sie verfügen über das Recht "Öffentlich bearbeiten". Benutzer, die über das Recht "Öffentlich bearbeiten" bei einer Funktion verfügen, können nur öffentliche Elemente für diese Funktion bearbeiten. Andere öffentliche Elemente sind schreibgeschützt. Schreibgeschützte Elemente sind dennoch nützlich, weil sie von Benutzern in die Baumgruppe "Eigene ..." kopiert und dort bearbeitet werden können.

Die Gruppe "Öffentlich" des Extras **Geplante Tasks** funktioniert ein bisschen anders. Alle Tasks in der Gruppe "Öffentlich" sind für Benutzer mit dem Recht "Bereitstellen" sichtbar, einschließlich Tasks zu Funktionen, auf die die Benutzer unter Umständen gar keinen Zugriff haben. Bearbeitet werden können jedoch nur diejenigen Tasks, für die die Benutzer über das Recht " Bereitstellen" verfügen. Die übrigen Tasks sind schreibgeschützt.

Wenn Sie über Rechte vom Typ "Öffentlich bearbeiten" und "Bereitstellen" verfügen, können Sie neue Tasks in der Gruppe "Öffentlich" erstellen sowie Tasks zu dieser Gruppe hinzufügen oder aus ihr löschen.

Referenz zu Konsolenrechten

Über die Konsolenrechte erhalten Sie Zugriff auf bestimmte Extras und Funktionen von Management Suite. Benutzer müssen über die erforderlichen Rechte verfügen, um entsprechende Aufgaben durchzuführen. Um beispielsweise Geräte im Bereich eines Benutzers remote zu steuern, muss ein Benutzer über das Remotesteuerungsrecht verfügen.

Die rollenbasierte Administration schließt folgende Berechtigungen ein:

- Administrator
- Agentenkonfiguration
- Alarmfunktion
- Einfache Webkonsole
- Inhaltsreplikation
- Coresynchronisierung
- Benutzerdefinierte Datenformulare
- Geräteverwaltung
    - Geräte hinzufügen oder löschen
    - Geräteüberwachung
    - Geräteenergieverwaltung
    - Lokale Benutzer und Gruppen verwalten

    - Öffentliche Gerätegruppen verwalten
    - Erkennung nicht verwalteter Geräte
- Inspector
- Linkmanagement
- Betriebssystembereitstellung - Versorgung
- Energieverwaltung
- Verwaltung öffentlicher Abfragen
- Bereiche aktualisieren
- Remotesteuerungsbefehle
    - Chat
    - Programme ausführen
    - Neustart
    - Remotesteuerung
    - Dateien übertragen
- Berichte
    - Berichtsdesigner
    - Berichte
- Sicherheit
    - Steuerung des Netzwerkzugriffs
    - Patch und Compliance
    - Sicherheitskonfigurationen
- Softwareverteilung
    - Verteilungsmethoden
    - Verzeichnisverwaltung
    - Verteilungspakete
    - Linkmanagement
    - Skripte verwalten
- Softwarelizenzüberwachung
- Benutzerverwaltung
- vPro

In den nachfolgenden Abschnitten erfahren Sie mehr über die einzelnen Berechtigungen und darüber, wie Sie mithilfe von Berechtigungen administrative Rollen erstellen können.

HINWEIS: Der Bereich steuert den Zugriff auf Geräte
Beachten Sie, dass beim Verwenden der Funktionen, die durch diese Berechtigungen freigegeben werden, die Benutzer stets durch ihren Bereich (die Geräte, die sie sehen und beeinflussen können) eingeschränkt sind.

Management Suite Administrator

Die Management Suite Administratorberechtigung gewährt Vollzugriff auf alle Anwendungstools (wobei die Verwendung dieser Extras jedoch immer noch auf die Geräte beschränkt ist, die zum Bereich des Administrators gehören).

Mit der Berechtigung eines Management Suite Administrators erhalten Benutzer folgende Möglichkeiten:

- Verwalten von Benutzern mit dem Extra "Benutzer".
- Anzeige und Konfiguration der Produktlizenzierung im Menü **Konfigurieren**.
- Konfigurieren von LANDesk Diensten.
- **WICHTIG:** Durchführung ALLER Management Suite Tasks, die durch die anderen unten aufgeführten Berechtigungen zugelassen sind.

Agentenkonfiguration

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra und alles andere sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles ändern. Kann keinen Agentenkonfigurationsjob bereitstellen.
- Bereitstellen: Kann alles sehen. Kann keine Änderungen vornehmen. Kann einen Zeitplan für alle Agentenkonfigurationstasks erstellen, die sichtbar sind (einschließlich "Öffentlich").
- Öffentlich bearbeiten: Kann Konfigurationen "Öffentlich" zuweisen. Kann öffentliche Konfigurationen bearbeiten.

Alarmfunktion

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra und alles andere sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles ändern. Kann nicht bereitstellen.
- Bereitstellen: Kann alles sehen. Kann keine Änderungen vornehmen. Kann bereitstellen.

Einfache Webkonsole

- Keine Rechte: Kann sich nicht bei der Webkonsole anmelden.
- Ansicht: Nicht zutreffend.
- Bearbeiten: Kann sich bei der Webkonsole anmelden und elementarste Dinge sehen.
- Bereitstellen: Nicht zutreffend.

Inhaltsreplikation

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra und alles andere sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles ändern.
- Bereitstellen: Nicht zutreffend.

Coresynchronisierung

- Keine Rechte: Kein Extra "Coresynchronisierung". Keine Kontextmenüoptionen für **Automatische Synchronisierung** oder **Auf Core(s) kopieren**. Import- und Exportoptionen werden dennoch angezeigt. (Diese sind in das Recht "Bearbeiten" des Extras eingebunden, das diese Optionen bereitstellt.)

- Ansicht: Kann das Extra sehen, aber keine Änderungen vornehmen. Immer noch keine Synchronisierungsoptionen in Kontextmenü, wie oben.
- Bearbeiten: Kann alles tun. Zielcores hinzufügen oder entfernen, Komponenten ein- und ausschalten, automatische Synchronisierung auf Instanzen aktivieren und manuelle Synchronisierung.
- Bereitstellen: Nicht zutreffend.

Benutzerdefinierte Datenformulare

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra und alles andere sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles ändern. Kann nicht bereitstellen.
- Bereitstellen: Kann alles sehen. Kann keine Änderungen vornehmen. Kann bereitstellen.

Geräteverwaltung

Geräte hinzufügen/löschen

- Keine Rechte:
  - Kann die Option **Neuen Computer einfügen** im Kontextmenü nicht sehen, wenn **Alle Geräte** in der **Netzwerkansicht** angezeigt werden.
  - Kann die Option **Löschen** im Kontextmenü nicht sehen, wenn ein Gerät in der **Netzwerkansicht** ausgewählt wird.
  - Kann den Baumknoten **Netzwerkansicht > Konfiguration > Vom Benutzer hinzugefügte Computer** nicht sehen.
- Ansicht: Nicht zutreffend.
- Bearbeiten:
  - Kann die Option **Neuen Computer einfügen** im Kontextmenü sehen und verwenden, wenn **Alle Geräte** in der **Netzwerkansicht** angezeigt werden.
  - Kann die Option **Löschen** im Kontextmenü sehen und verwenden, wenn ein Gerät in der **Netzwerkansicht** ausgewählt wird.
  - Kann den Baumknoten **Netzwerkansicht > Konfiguration > Vom Benutzer hinzugefügte Computer** sehen.
- Bereitstellen: Nicht zutreffend.

Geräteüberwachung

- Keine Rechte: Kann **Geräteüberwachung** im Menü **Konfigurieren** nicht sehen.
- Ansicht: Kann die Extras "Alarmierung" und "Protokolle" sehen. Kann Informationen im Extra "Geräteüberwachung" sehen. Kann diese nicht bearbeiten.
- Bearbeiten: Kann die Extras "Alarmierung" und "Protokolle" sehen. Kann Informationen im Extra "Geräteüberwachung" sehen und bearbeiten.
- Bereitstellen: Nicht zutreffend.

Geräteenergieverwaltung

- Bearbeiten: Kann bei der Auswahl eines Geräts die Optionen **Reaktivieren**, **Neu starten** und **Herunterfahren** im Kontextmenü sehen und verwenden.

Lokale Benutzer und Gruppen verwalten

- Bearbeiten: Kann bei der Auswahl eines Geräts die Option **Lokale Benutzer und Gruppen verwalten** im Kontextmenü sehen und verwenden.

Öffentliche Gerätegruppen verwalten

- Keine Rechte: Kann keine Änderungen unter **Öffentliche Geräte** vornehmen.
- Ansicht: Nicht zutreffend.
- Bearbeiten: Nicht zutreffend.
- Bereitstellen: Nicht zutreffend.
- Öffentlich bearbeiten: Kann Gerätegruppen in **Öffentliche Geräte** erstellen, löschen und ändern. Kann eine Gerätegruppe in **Öffentliche Geräte** verschieben.

Erkennung nicht verwalteter Geräte

- Keine Rechte: Kann das Extra "UDD" nicht sehen.
- Ansicht: Kann das Extra "UDD" öffnen und alle Elemente sehen. Kann nichts erstellen, löschen oder bearbeiten.
- Bearbeiten: Kann das Extra "UDD" öffnen und alle Elemente sehen. Kann alles erstellen, löschen oder bearbeiten.
- Bereitstellen: Kann das Extra "UDD" öffnen und alle Elemente sehen. Kann nichts erstellen, löschen oder bearbeiten. Kann einen UDD-Task planen.

Inspector

- Keine Rechte: Kann das Extra "Inspector" nicht sehen.
- Ansicht: Kann das Extra "Inspector" öffnen und alle Elemente sehen.

Betriebssystembereitstellung / Versorgung

- Keine Rechte: Kann das Extra zur Betriebssystembereitstellung nicht sehen.
- Ansicht: Kann das Extra sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann Elemente erstellen, bearbeiten und löschen. Kann keinen Zeitplan für Tasks erstellen.
- Bereitstellen: Kann Zeitpläne für Tasks erstellen, die angezeigt werden (einschließlich "Öffentlich"). Kann keine Elemente erstellen, bearbeiten und löschen.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Energieverwaltung

- Keine Rechte: Kann das Extra zur Energieverwaltung nicht sehen.
- Ansicht: Kann das Extra sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann Elemente erstellen, bearbeiten und löschen. Kann keinen Zeitplan für Tasks erstellen.
- Bereitstellen: Kann Zeitpläne für Tasks erstellen, die angezeigt werden (einschließlich "Öffentlich"). Kann keine Elemente erstellen, bearbeiten und löschen.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Verwaltung öffentlicher Abfragen

- Keine Rechte: Normales Verhalten.
- Ansicht: Nicht zutreffend.
- Bearbeiten: Nicht zutreffend.

- Bereitstellen: Nicht zutreffend.
- Öffentlich bearbeiten: Kann Abfragen in den Ordner "Öffentlich" verschieben. Kann Abfragen im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Bereiche aktualisieren

- Keine Rechte: Die Symbolleisten-Schaltfläche **Bereiche aktualisieren** in der **Netzwerkansicht** erfüllt keinerlei Funktion.
- Bearbeiten: Die Symbolleisten-Schaltfläche **Bereiche aktualisieren** in der **Netzwerkansicht** aktualisiert alle Bereiche. Diese Schaltfläche verwenden Sie, wenn Sie Geräte zu einem Bereich hinzugefügt haben oder den Bereich eines Benutzers geändert haben und möchten, dass der Benutzer den neuen Bereich sehen kann. Ansonsten kann es bis zu einer Stunde dauern, bis die Aktualisierung des Bereichs automatisch erfolgt.

Remotesteuerungsbefehle

Chat

- Bearbeiten: Kann die Option **Remotesteuerung > Chat** sehen und verwenden. Die Option **Chat** ist im Fenster "Remotesteuerung" aktiviert.

Programme ausführen

- Bearbeiten: Kann die Option **Remotesteuerung > Programm ausführen** sehen und verwenden. Die Option **Programm ausführen** ist im Fenster "Remotesteuerung" aktiviert.

Neustart

- Bearbeiten: Kann die Option **Remotesteuerung > Neustart** sehen und verwenden. Die Option **Neustart** ist im Fenster "Remotesteuerung" aktiviert.

Remotesteuerung

- Keine Rechte: Kann die Option **Remotesteuerung > Remotesteuerung** im Kontextmenü nicht sehen.
- Ansicht: Kann die Option **Remotesteuerung > Remotesteuerung** sehen und ein Gerät remote steuern. Kann die Steuerung des Geräts nicht übernehmen (nur Anzeigen).
- Bearbeiten: Kann die Option **Remotesteuerung > Remotesteuerung** sehen, ein Gerät remote steuern und dessen Steuerung übernehmen.
- Bereitstellen: Nicht zutreffend.

Dateien übertragen

- Bearbeiten: Kann die Option **Remotesteuerung > Dateien übertragen** sehen und verwenden. Die Option **Dateien übertragen** ist im Fenster "Remotesteuerung" aktiviert.

Berichte

Berichtsdesigner

- Keine Rechte: Kann den Designer nicht öffnen.
- Ansicht: Nicht zutreffend.
- Bearbeiten: Kann den Designer öffnen und Berichte erstellen oder bearbeiten.
- Bereitstellen: Nicht zutreffend.
- Öffentlich bearbeiten: Nicht zutreffend.

Berichte

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra sehen und Berichte anzeigen. Kann Berichte ausführen. Kann keinerlei Änderungen vornehmen.
- Bearbeiten: Kann Berichte anzeigen und Berichtseigenschaften ändern. Dieses Recht alleine gewährt keinen Zugriff auf den Designer. Für den Zugriff auf den Berichtsdesigner ist das Recht "Bearbeiten" erforderlich.
- Bereitstellen: Kann Bericht planen und veröffentlichen.
- Öffentlich bearbeiten: Kann Berichte in die Gruppe "Öffentlich" verschieben.

Sicherheit

Steuerung des Netzwerkzugriffs

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra und alles andere sehen (so wie etwa die 802.1x-Konfiguration). Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und ändern, einschließlich der NAC-Einstellungen.
- Bereitstellen: Nicht zutreffend.

Patch und Compliance

- Keine Rechte: Kann das Extra nicht sehen. Kann keinerlei geplante Tasks oder Richtlinien in der Softwareverteilung sehen, die über das Extra erstellt wurden.
- Ansicht: Kann das Extra sehen. Kann alles innerhalb des Extras sehen. Kann keine Inhalte downloaden, keine Konfigurationen erstellen, bearbeiten oder löschen oder irgendwelche Änderungen vornehmen. Der Zugriff ist schreibgeschützt.
- Bearbeiten: Kann das Extra sehen. Kann alles innerhalb des Extras sehen. Kann alles bearbeiten. Kann nichts planen, keine Downloads von Inhalten, keine Scanjobs oder Reparaturjobs, keine Verlaufsdaten sammeln usw.
- Bereitstellen: Kann das Extra sehen. Kann alles innerhalb des Extras sehen. Kann nichts ändern, kann aber einen Task oder eine Richtlinie unter Verwendung der Informationen zu sichtbaren Elementen (einschließlich "Öffentlich") erstellen.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Sicherheitskonfigurationen

- Keine Rechte: Kann das Extra nicht sehen. Kann keinerlei geplante Tasks oder Richtlinien im Fenster "Geplante Tasks" sehen, die über dieses Extra erstellt wurden.
- Ansicht: Kann dieses Extra und das Extra "Sicherheitsaktivitäten" sehen. Kann Konfigurationen zwar anzeigen, aber nicht ändern und auch keine Tasks erstellen.
- Bearbeiten: Kann dieses Extra und das Extra "Sicherheitsaktivitäten" sehen. Kann alles innerhalb des Extras sehen. Kann alles bearbeiten. Kann keinen Zeitplan erstellen.
- Bereitstellen: Kann dieses Extra und das Extra "Sicherheitsaktivitäten" sehen. Kann alles innerhalb des Extras sehen. Kann nichts ändern, kann aber einen Task oder eine Richtlinie zur Bereitstellung für einen Client erstellen oder die Konfiguration für sichtbare Elemente (einschließlich "Öffentlich") ändern.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Softwareverteilung

Verteilungsmethoden

- Ansicht: Kann das Extra und dessen gesamten Inhalt sehen.
- Bearbeiten: Kann Methoden erstellen, bearbeiten oder löschen.
- Bereitstellen: Nicht zutreffend.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Verzeichnisverwaltung

- Ansicht: Kann das Extra und dessen gesamten Inhalt sehen (unter der Annahme, dass bereits eine Authentifizierung erfolgt ist).
- Bearbeiten: Kann sich bei einem neuen Verzeichnis authentifizieren und alles sehen sowie Abfragen erstellen, bearbeiten oder löschen.
- Bereitstellen: Nicht zutreffend.

Verteilungspakete

- Ansicht: Kann das Extra und dessen gesamten Inhalt sehen.
- Bearbeiten: Kann Pakete erstellen, bearbeiten oder löschen.
- Bereitstellen:
  - Kann ein Paket im Extra "Verteilungspaket" erstellen.
  - Kann die Schaltfläche **Softwareverteilung** im Extra "Geplante Tasks" verwenden.
  - Kann die Schaltfläche **Benutzerdefinierte Skripts erstellen** im Extra "Geplante Tasks" verwenden.
  - Dies gilt für alle Elemente, die sichtbar sind (einschließlich "Öffentlich").
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Linkmanagement

- Keine Rechte: Kann das Extra zum Linkmanagement nicht sehen.
- Ansicht: Kann das Extra sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann Elemente erstellen, bearbeiten und löschen. Kann weder für Tasks noch für Richtlinien einen Zeitplan erstellen.
- Bereitstellen: Kann keine Elemente erstellen, bearbeiten und löschen. Kann für Tasks und Richtlinien einen Zeitplan erstellen.

Skripte verwalten

- Ansicht: Kann dieses Extra und alles andere sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles ändern. Kann keine Zeitplanung für Tasks vornehmen.
- Bereitstellen: Kann Zeitpläne für Tasks zu Elementen erstellen, die sichtbar sind (einschließlich "Öffentlich"). Kann keine Elemente erstellen, bearbeiten und löschen.
- Öffentlich bearbeiten: Kann Elemente in den Ordner "Öffentlich" verschieben. Kann Elemente im Ordner "Öffentlich" erstellen, bearbeiten oder löschen.

Softwarelizenzüberwachung

- Keine Rechte: Kann das Extra "Softwarelizenzüberwachung" nicht sehen.
- Ansicht: Kann alles sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Kann alles sehen und alles bearbeiten.
- Bereitstellen: Nicht zutreffend.

Benutzerverwaltung

- Keine Rechte: Kann das Extra "Benutzer" nicht sehen.
- Ansicht: Kann alles sehen. Kann keine Änderungen vornehmen.
- Bearbeiten: Nicht zutreffend.
- Bereitstellen: Nicht zutreffend.

vPro

- Keine Rechte: Kann vPro-Informationen und -Einstellungen weder anzeigen noch ändern.
- Ansicht: Nicht zutreffend.
- Bearbeiten: Kann vPro-Informationen und -Einstellungen anzeigen und ändern.
- Bereitstellen: Nicht zutreffend.

Zusätzliche Informationen zu geplanten Tasks

- Benutzer, die Rechte zum "Bereitstellen" für ein Extra haben, das Tasks verwendet, die geplant werden können, können das Extra "Geplanter Task" sehen.
- Wer Rechte zum "Bereitstellen" hat, besitzt auch das Recht, einen beliebigen Teil eines Tasks zu ändern, für dessen Typ Rechte zum "Bereitstellen" vorliegen (wie beispielsweise die Agentenkonfiguration, Softwareverteilung, Patch usw.)
- Wer Rechte zum "Bereitstellen" hat, kann nur die Bereiche **Ziel** und **Zeitplan** eines öffentlichen Tasks ändern.
- Wer die Rechte "Bereitstellen" und "Öffentlich bearbeiten" besitzt, kann beliebige Änderungen an öffentlichen Tasks vornehmen und Tasks in öffentliche Ordner oder aus diesen heraus verschieben.
- Wer über das Recht "Öffentlich bearbeiten" verfügt, aber nicht über das Recht "Bereitstellen", kann keinen Task diesen Typs bearbeiten, öffentliche Tasks eingeschlossen.

Erstellen von Bereichen

Ein Bereich definiert die Geräte, die von einem Management Suite Benutzer angezeigt und verwaltet werden können.

Ein Bereich kann beliebig groß oder klein sein, alle in eine Coredatenbank gescannten verwalteten Geräte umfassen oder sich nur auf ein einziges Gerät erstrecken. Diese Flexibilität, kombiniert mit dem modularen Toolzugriff, macht aus der rollenbasierten Administration eine vielseitige Verwaltungsfunktion.

Standardbereiche

Die rollenbasierte Administration von Management Suite umfasst einen Standardbereich: "Alle Geräte" Dieser Bereich umfasst alle verwalteten Geräte in der Datenbank. Sie können den Standardbereich weder bearbeiten noch entfernen.

Benutzerdefinierte Bereiche

Es gibt drei verschiedene benutzerdefinierte Bereiche, die Sie erstellen und Benutzern zuweisen können:

- **LDMS Abfrage:** Beschränkt den Zugriff auf diejenigen Geräte, die einer benutzerdefinierten Abfragesuche entsprechen. Um einen Bereich zu definieren, können Sie eine vorhandene Abfrage auswählen oder im Dialogfeld "Bereichseigenschaften" neue Abfragen erstellen. Beachten Sie, dass Sie auch Abfragen aus der Gruppe **Abfragen** der Netzwerkansicht direkt in die Gruppe **Bereiche** kopieren können. Weitere Informationen zum Erstellen von Abfragen finden Sie unter "Abfragen/Verzeichnis-Manager" auf Seite 193.
- **LDAP:** Steuert den Zugriff auf lediglich diejenigen der vom Inventarscanner erfassten Geräte, die sich in einer LDAP-konformen Verzeichnisstruktur befinden. Wählen Sie Verzeichnispfade im Dialogfeld **Sichtbare Geräte auswählen** aus, um einen Bereich zu definieren. Dieser verzeichnisbasierte Bereichstyp unterstützt auch benutzerdefinierte Verzeichnisstandorte (wenn Sie einen benutzerdefinierten Verzeichnispfad als Teil einer Agentenkonfiguration eingegeben haben). Verfügbare benutzerdefinierte Verzeichnispfade werden im Dialogfeld **Sichtbare Geräte auswählen** angezeigt. Verwenden Sie benutzerdefinierte Verzeichnisse, um einen Bereich zu definieren, wenn Ihr System nicht über eine Active Directory- oder NetWare eDirectory LDAP-kompatible Struktur verfügt, oder wenn Sie den Zugriff auf Geräte über ein bestimmtes organisatorisches Detail, z. B. einen Standort oder eine Abteilung, beschränken möchten.
- **Gruppe "Gerät":** Kontrolliert den Zugriff nur auf die Geräte, die zu einer bestimmten Gerätegruppe gehören.

Sie können einem Benutzer von Management Suite jeweils einen oder mehrere Bereiche zuweisen. Darüber hinaus kann ein Bereich mit mehreren Benutzern verknüpft sein.

So funktioniert die Verknüpfung mit mehreren Bereichen

Sie können jedem Benutzer von Management Suite nach Bedarf mehrere Bereiche zuweisen. Wenn einem Benutzer mehrere Bereiche zugewiesen werden, hat der Benutzer Rechte auf allen Computern in allen zugewiesenen Bereichen. Die kumulative Liste der Computer aus allen zugewiesenen Bereichen stellt den tatsächlichen Bereich des Benutzers dar.

Der tatsächliche, zusammengefasste Bereich eines Benutzers kann jederzeit durch Hinzufügen oder Entfernen von Bereichen geändert werden. Mehrere Bereiche und Bereichstypen können miteinander kombiniert werden.

Die Rechte und Bereiche eines Benutzers können jederzeit geändert werden. Wenn Sie die Rechte oder Bereiche eines Benutzers ändern, werden diese Änderungen bei der nächsten Anmeldung des Benutzer an der Konsole wirksam oder wenn ein Konsolenadministrator auf der Konsole (ganz oben im Fenster) auf die Symbolleisten-Schaltfläche **Bereich aktualisieren** klickt.

Erstellen eines Bereichs

Ein Bereich definiert die Geräte, die von einem Management Suite Benutzer angezeigt und verwaltet werden können.

Ein Bereich kann beliebig groß oder klein sein, alle in eine Coredatenbank gescannten verwalteten Geräte umfassen oder sich nur auf ein einziges Gerät erstrecken.

So erstellen Sie einen Bereich

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf **Bereiche** und wählen Sie **Neuer Bereich** aus.
3. Geben Sie im Dialogfeld **Bereichseigenschaften** einen Namen für den neuen Bereich ein.
4. Geben Sie an, welche Art von Bereich Sie erstellen möchten (LDMS Abfrage, LDAP Verzeichnis oder benutzerdefiniertes Verzeichnis oder Gerätegruppe), indem Sie auf einen Bereichstyp in der Dropdownliste klicken und dann auf **Neu** klicken.
5. Wenn Sie einen Bereich erstellen, der auf einer LDMS Abfrage basiert, definieren Sie die Abfrage im Dialogfeld **Neue Bereichsabfrage** und klicken dann auf **OK**.
6. Wenn Sie einen verzeichnisbasierten Bereich erstellen, wählen Sie Speicherorte (LDAP-Verzeichnis und/oder benutzerdefiniertes Verzeichnis) aus der Liste **Sichtbare Geräte auswählen** aus (das Verzeichnis können Sie durchsuchen, indem Sie auf **Verzeichnis durchsuchen** klicken) und klicken Sie dann auf **OK**.

Klicken Sie auf das Plus- (+) oder das Minuszeichen (-), um Knoten in der Verzeichnisstruktur zu erweitern oder zu reduzieren. Alle Knoten unter einem ausgewählten übergeordneten Knoten sind im Bereich enthalten.

LDAP-Verzeichnisse werden durch den Active Directory- oder den eDirectory-Speicherort eines Servers bestimmt. Benutzerdefinierte Verzeichnisspeicherorte werden bestimmt durch das Computerstandort-Attribut eines Geräts in der Inventardatenbank. Dieses Attribut wird während der Agentenkonfiguration definiert.

7. Wenn Sie einen gerätebasierten Bereich erstellen, wählen Sie eine Gruppe aus der Liste mit den verfügbaren Gerätegruppen aus und klicken dann auf **OK**.
8. Klicken Sie auf **OK**, um den Bereich zu speichern und das Dialogfeld zu schließen.

So erstellen Sie einen Bereich, der auf einer vorhandenen Abfrage basiert

1. Klicken Sie mit der rechten Maustaste auf **Bereiche** und wählen Sie **Neuer Bereich aus Abfrage** aus.
2. Wählen Sie die gewünschten Abfrage aus und klicken Sie auf **OK**.
3. Es wird eine Kopie der Abfrage erstellt und ein neuer Bereich wird im Baum anzeigt, wobei der Name des Bereichs auf dem Namen der Quellabfrage basiert.

HINWEIS: Sie können von einer vorhandenen Abfrage aus sehr schnell einen Bereich erstellen, indem Sie eine Abfrage aus der Netzwerkansicht ziehen und auf dem Baum "Bereiche" ablegen.

HINWEIS: Bereiche verwenden eine Kopie der Abfrage, auf der sie basieren. Änderungen, die für die Quellabfrage in der Netzwerkansicht vorgenommen werden, haben keinerlei Auswirkungen auf vorhandene Bereiche.

Informationen zum Dialogfeld "Bereichseigenschaften"

Mit diesem Dialogfeld erstellen oder bearbeiten Sie einen Bereich. Sie können auf dieses Dialogfeld zugreifen, indem Sie einen Bereich auswählen und in der Symbolleiste auf die Schaltfläche **Bereich bearbeiten** klicken, oder indem Sie mit der rechten Maustaste auf den Bereich und dann auf **Eigenschaften** klicken.

- **Bereichsname:** Identifiziert den Bereich.
- **Bereichstyp auswählen:**

- **LDMS Abfrage:** Erstellt einen Bereich, dessen Gerätebereich durch eine benutzerdefinierte Abfrage bestimmt wird. Wenn dieser Bereichstyp ausgewählt ist, wenn Sie auf **Neu** klicken, wird das Dialogfeld **Neue Abfrage** geöffnet, in dem Sie eine Abfrage definieren und speichern können. Dasselbe Dialogfeld wird angezeigt, wenn Sie eine Datenbankabfrage in der Netzwerkansicht erstellen. (Beachten Sie, dass Sie Abfragen auch aus der Gruppe **Abfragen** in der Netzwerkansicht direkt in die Gruppe **Bereiche** kopieren können.)
- **LDAP:** Erstellt einen Bereich, dessen Gerätebereich vom Gerätestandort (LDAP-Verzeichnis und/oder benutzerdefiniertes Verzeichnis) bestimmt wird. Wenn dieser Bereichstyp ausgewählt ist, wenn Sie auf **Neu** klicken, wird das Dialogfeld **Sichtbare Geräte auswählen** geöffnet, in dem Sie Speicherorte aus Inventardaten auswählen können. Klicken Sie auf das Plus- (+) oder das Minuszeichen (-), um Knoten in der Verzeichnisstruktur zu erweitern oder zu reduzieren. Mit Strg + Mausklick können Sie mehrere Speicherorte auswählen. Alle Knoten unter einem ausgewählten übergeordneten Knoten sind im Bereich enthalten. Wenn Sie auf **Verzeichnisse durchsuchen** klicken, können Sie Geräte aus dem aktiven LDAP-Verzeichnisbaum für die von Ihnen konfigurierten Verzeichnisse durchsuchen und auswählen.
- **Gruppe "Gerät":** Erstellt einen Bereich, dessen Spektrum durch eine vorhandene Gerätegruppe bestimmt wird, die unter dem Objekt "Geräte" in der Netzwerkansicht zu finden ist. Wenn dieser Bereichstyp ausgewählt ist, wenn Sie auf **Neu** klicken, wird das Dialogfeld **Abfragefilter** geöffnet, in dem Sie eine Gerätegruppe auswählen können.

- **Aktuelle Bereichsdefinition:** Zeigt die Abfrageanweisungen für einen abfragebasierten Bereich an, die Speicherortpfade für einen verzeichnisbasierten Bereich oder den Gruppennamen für eine Gerätegruppen-basierten Bereich.
- **Bearbeiten:** Öffnet das relevante Dialogfeld des Bereichs, um Ihnen die Möglichkeiten zum Ändern der Abfrageparameter und Befehle zu geben.

Erstellen eines Teams

Ein rollenbasiertes Verwaltungsteam ist eine Gruppe von Benutzern, die gemeinsam Eigentümer aller dem Team gehörenden Tasks und Konfigurationen sind und diese anzeigen können.

So erstellen Sie ein Team

1. Klicken Sie im Extra **Benutzerverwaltung** mit der rechten Maustaste auf **Teams** und klicken Sie dann auf **Neues Team**.
2. Geben Sie einen Team**namen** ein.
3. Wählen Sie die **Benutzer** und Gruppen aus, die dem Team angehören sollen.
4. Klicken Sie auf **OK**.

Verwenden von Teams

Ein rollenbasiertes Verwaltungsteam ist eine Gruppe von Benutzern, die gemeinsam Eigentümer aller dem Team gehörenden Tasks und Konfigurationen sind und diese anzeigen können. Wenn Sie beispielsweise mehrere Abteilungen haben, die Abfragen oder Task gemeinsam benutzen sollen, können Sie diese Abteilungen zu einem Team gruppieren. Die Tasks und Konfigurationen eines Teams erscheinen in der Baumansicht eines Extras in einer speziellen Gruppe, die nach dem Team benannt ist. Angenommen, Sie haben ein Team namens "Salt Lake", bei dem Sie Mitglied sind, dann würden Sie in der **Netzwerkansicht** unter der Gruppe **Geräte** eine Untergruppe "'Salt Lake'-Geräte" sehen. Einzelpersonen können mehreren Teams angehören.

Personen, die nicht Mitglied eines bestimmten Teams sind, können die Gruppe dieses Teams nirgends in der Konsole sehen. Personen mit den Rechten eines Administrators können alle Teams und sämtliche Inhalte der Teams sehen. Zwar können Sie öffentliche Ordner dazu verwenden, Konsoleninhalte gemeinsam zu benutzen, doch sind Inhalte von öffentlichen Ordner für jeden Benutzer mit Rechten für ein Extra sichtbar. Der Vorteil von Teams besteht darin, dass nur Mitglieder des Team Teaminhalte sehen können, was unter Umständen dazu beiträgt, dass Inhalte besser organisiert und damit für das Team besser zugänglich gemacht werden.

Teams umfassen eine oder mehrere Gruppenberechtigungen. Sie können sogar Teams mit nur einer Person oder nur zwei Personen erstellen. Wenn sich beispielsweise eine Person krank gemeldet hat, können Sie die Vertretung dieser Person zum selben Team hinzufügen. Oder falls zwei Personen dieselben Verantwortlichkeiten haben, können Sie sie in ein Team stellen.

Administratoren und Teammitglieder können den Eigentümer von Elementen in der Baumstruktur ändern, indem sie mit der rechten Maustaste darauf klicken und dann **Info** auswählen. Dialogfelder vom Typ "Informationen" weisen eine Dropdownliste **Eigentümer** auf, in der Sie den Eigentümer des Elements auswählen können.

Verwenden der Zeitbeschränkungen für die Remotesteuerung

Mit diesen Zeitbeschränkungen für die Remotesteuerung wird die Anzahl der Stunden und Tage beschränkt, während derer Benutzer Remotesteuerungssitzungen initiieren können. Sie können die Wochentage und die Start- und Endzeit (im UTC-Format) angeben, während derer Sie die Remotesteuerung zulassen wollen.

Beachten Sie, dass die Startzeit im UTC-Format (Coordinated Universal Time, Koordinierte Weltzeit oder Greenwich Mean Time (GMT)) angegeben wird. Der Coreserver bestimmt die Startzeit, indem er die vom Betriebssystem des Coreservers gemeldete UTC-Zeit überprüft. Der Coreserver nimmt keine Anpassung bezüglich der lokalen Zeitzone der Konsolenbenutzer vor. Bei der Eingabe des Startzeitwerts müssen Sie die Differenz zwischen der UTC-Zeit und der lokalen Zeitzone des Konsolenbenutzers kompensieren und die sich daraus ergebende angepasste Zeit verwenden.

Standardmäßig sind keine Zeitbeschränkungen für die Remotesteuerung aktiv.

Beachten Sie, dass RBA-Rechte additiv sind. Wenn ein Benutzer Mitglied mehrerer Rollen ist, könnte es sein, dass Sie unbeabsichtigterweise Remotesteuerung zulassen, wenn Sie diese eigentlich beschränken wollten.

Wenn beispielsweise ein Benutzer Mitglied einer Remotesteuerungsrolle ist, für die Zeitbeschränkungen gelten, und dieser Benutzer ist gleichzeitig Mitglied einer Sicherheitsrolle, für die keine Zeitbeschränkungen definiert sind, dann gelten für diesen Benutzer keinerlei Zeitbeschränkungen.

Um sicherzustellen, dass Zeitbeschränkungen für die Remotesteuerung auch so zur Anwendung kommen, wie Sie dies beabsichtigen, sollten Sie sicherstellen, dass Benutzern mit Zeitbeschränkungen nur eine einzige Rolle zugewiesen ist.

Zuweisen von Zeitbeschränkungen für die Remotesteuerung

Mit diesen Zeitbeschränkungen für die Remotesteuerung wird die Anzahl der Stunden und Tage beschränkt, während derer Benutzer Remotesteuerungssitzungen initiieren können.

So verwenden Sie die Zeitbeschränkungen für die Remotesteuerung

1. Klicken Sie mit der rechten Maustaste im Extra "Benutzerverwaltung" (**Extras > Administration > Benutzerverwaltung**) auf einen Benutzer oder eine Gruppe im Baum **Benutzer und Gruppen** und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im linken Fensterausschnitt auf **RC-Zeitbeschränkungen**.
3. Aktivieren Sie die Option **Uhrzeitbeschränkungen verwenden**.
4. Markieren Sie die Tage, die aktiviert werden sollen.
5. Geben Sie den UTC-Zeitbereich ein, während dem Sie Remotesteuerung zulassen wollen.
6. Klicken Sie abschließend auf **OK**.

Corekonfiguration

Wahl der Hardware für den Coreserver und die Datenbank

Bei der Einrichtung eines LANDesk Management Suite Coreservers müssen Entscheidungen bezüglich Geschwindigkeit, Speicher und Plattenspeicher für die beteiligten Server getroffen werden. Der Administrator muss außerdem entscheiden, zu welchem Zeitpunkt eine Umstieg von einem Coreserver auf mehrere Coreserver erfolgen muss. Dieser Abschnitt befasst sich mit diesen Entscheidungen. Bei der Hardware betreffen die vier wesentlichen Entscheidungen die Wahl der CPU, des Hauptspeichers, des Plattenspeichers und der Netzwerkkarte. Die nachstehende Liste bietet Hardwareempfehlungen für unterschiedliche Anzahlen von verwalteten Knoten.

Der wichtigste Faktor bei der Entscheidungsfindung ist die Anzahl der verwalteten Knoten im Netzwerk. Die Anzahl der Knoten sollte bereits bei der Erfassung von Netzwerkinformationen geschätzt worden sein. Es gibt aber noch andere Faktoren, die berücksichtigt werden sollten, wie etwa welche Komponenten am meisten verwendet werden, wie viele Personen Zugriff auf die LANDesk Konsole oder die Webkonsole benötigen, welches Network Management-Modell verwendet werden soll und wie Konformität oder "Compliance" mit Geschäftspraktiken und Standards erreicht wird.

Für jede Umgebung gelten andere Hardwareempfehlungen, und die nachstehenden Empfehlungen sind als allgemeine Richtlinien zu verstehen, die Sie bei der Wahl der idealen Hardware für eine bestimmte Umgebung unterstützen sollen.

Bei der Datenbanksoftware werden die folgenden Optionen unterstützt:

- Microsoft SQL Express 2008 (im Lieferumfang von Management Suite enthalten, aber nur für Testumgebungen und für Bereitstellungen in kleinem Rahmen empfohlen)
- Microsoft SQL 2005
- Microsoft SQL 2008
- Oracle 11g R2

Corekonfigurationen mit einem einzelnen Server

Alle Management Suite-Dienste auf einem Server (bis zu 750 Geräte)

Für Management Suite-Verwaltungsdomänen mit 750 oder weniger Geräten können Sie den Coreserver, die Konsole, den Webkonsolenserver und die Coredatenbank auf einem Server installieren. Bei diesen Gegebenheiten empfiehlt es sich, die Microsoft SQL Express-Standarddatenbank zu verwenden, die in der Regel einfacher zu verwalten ist. Bevor Sie Management Suite in einer Konfiguration mit bis zu 1.000 Geräten installieren, sollten Sie sicherstellen, dass Ihr Server mindestens folgende Systemanforderungen erfüllt:

- Intel Xeon Dual Core 32-Bit oder 64-Bit-Prozessor
- 4 GB RAM
- 100/1000-Megabit-Netzwerkadapter
- 72 GB freier Speicherplatz auf Festplatten oder Arrays mit mindestens 10.000 U/min.

WICHTIG: Die maximale Größe einer Microsoft SQL Express-Datenbank beträgt 4 Gigabyte. Sobald dieser Grenzwert erreicht ist, arbeitet der Coreserver nicht mehr ordnungsgemäß und die Datenbank kann keine

weiteren Daten mehr speichern. Jeder einzelne Agent kann durchaus 2 bis 4 Megabyte oder mehr Speicher beanspruchen, daher sollten Sie die Speicherplatzverwendung überwachen und ein Upgrade auf die Vollversion von SQL vornehmen, bevor der Grenzwert von 4 Gigabyte erreicht ist.

Konfiguration auf einzelnem Server (750 bis 1.500 Geräte)

Ein Server genügt auch noch, wenn die Management Suite-Verwaltungsdomäne 750 bis 1.500 Geräte umfasst. Stellen Sie vor der Installation von Management Suite sicher, dass der Server die folgenden Systemanforderungen erfüllen.

- Intel Xeon Dual Core 64-Bit-Prozessor
- Mindestens 4 GB RAM
- 1 GB Netzwerkadapter
- 3 Laufwerke oder Arrays mit 72 GB freiem Plattenspeicher pro Array mit einer Geschwindigkeit von mindestens 15.000 U/min.

HINWEIS: Bei einem Coreserver mit 750 bis 1.500 Knoten, auf dem sämtliche LANDesk Funktionen ausgeführt werden, können sich die Schreib-/Lesevorgänge verlangsamen, wenn sich das Betriebssystem, die LANDesk Management Suite-Anwendung, die Datenbankanwendung und die Datenbankprotokolle allesamt auf demselben Laufwerk oder Array befinden. Hier muss unter Umständen die Konfiguration optimiert werden. Für einen Server, der eine solch umfassende Konfiguration hostet, werden drei Laufwerksarrays mit separaten Spindeln (physikalischen Laufwerken) empfohlen, um Ressourcenprobleme zu vermeiden. Die folgenden Laufwerkskonfigurationen sollten implementiert werden.

- Ein Laufwerk oder Array für das Betriebssystem
- Ein Laufwerk oder Array für die LANDesk Management Suite-Anwendung und die Datenbankanwendung
- Ein Laufwerk oder Array für die Datenbank und die Datenbankprotokolle

HINWEIS: Der Server, auf dem sich diese Konfiguration befindet, erfordert drei Arrays auf separaten Spindeln (physikalischen Laufwerken).

Konfiguration auf einzelnem Server (1.500 bis 3.000 Geräte)

Ein Server genügt auch noch, wenn die Management Suite-Verwaltungsdomäne 1.500 bis 3.000 Geräte umfasst. Stellen Sie vor der Installation von Management Suite sicher, dass der Server die folgenden Systemanforderungen erfüllen.

- Dual Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. zwei physikalische Prozessoren)
- 6 bis 10 GB RAM oder mehr (4 GB für das Betriebssystem und die LANDesk Dienste, plus 1 bis 2 MB pro Knoten für die Datenbank. Plus 10 GB RAM als Reserve.)
- Wichtig: Der Management Suite-Coreserver in dieser Konfiguration erfordert zwei Laufwerkarrays auf separaten Spindeln.
- 1 GB Netzwerkadapter
- 3 Laufwerke oder Arrays mit 72 GB freiem Plattenspeicher pro Array mit einer Geschwindigkeit von mindestens 15.000 U/min.

HINWEIS: Bei einem Coreserver mit 1.500 bis 3.000 Knoten, auf dem sämtliche LANDesk Funktionen ausgeführt werden, können sich die Schreib-/Lesevorgänge verlangsamen, wenn sich das Betriebssystem, die LANDesk Management Suite-Anwendung, die Datenbankanwendung und die Datenbankprotokolle allesamt auf demselben Laufwerk oder Array befinden. Hier muss unter Umständen die Konfiguration optimiert werden. Für einen Server, der eine solch umfassende Konfiguration hostet, werden drei Laufwerksarrays mit separaten Spindeln (physikalischen Laufwerken) empfohlen, um Ressourcenprobleme zu vermeiden. Die folgenden Laufwerkskonfigurationen sollten implementiert werden.

- Ein Array für das Betriebssystem, RAID 0, RAID 1, RAID 5 oder gleichwertige/schnellere Technologie.
- Die Management Suite-Software sollte auf einem Array mit RAID 0, RAID 5, RAID 10 oder gleichwertiger/schnellerer Technologie installiert werden.
- Ein Array für die Datenbank und die Datenbankprotokolle, RAID 0, RAID 5 oder RAID 10 oder gleichwertige/schnellere Technologie.

WICHTIG: Der Server, auf dem sich diese Konfiguration befindet, erfordert drei Arrays auf separaten Spindeln (physikalischen Laufwerken).

Corekonfigurationen mit mehreren Servern

Konfiguration mit mehreren Servern (3.000 bis 5.000 Geräte)

Wenn die Management Suite-Verwaltungsdomäne 3.000 bis 5.000 Geräte umfasst, empfiehlt LANDesk, die Management Suite-Komponenten auf zwei Server aufzuteilen, um eine bessere Datenbankperformance zu erzielen. Stellen Sie vor der Installation von Management Suite sicher, dass die Server die folgenden Systemanforderungen erfüllen.

Management Suite-Coreserver und Webkonsolensoftware auf einem Server

- Dual Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. zwei physikalische Prozessoren)
- Mindestens 4 GB RAM
- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)
- Zwei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min
- Das Betriebssystemarray sollte RAID 0 oder RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Die Management Suite-Software sollte auf einem Array mit RAID 0, RAID 5 oder RAID 10 oder gleichwertiger/schnellerer Technologie installiert werden.

Coredatenbank auf einem zweiten Server

- Für den Datenbankserver wird ein 64-Bit-Betriebssystem zur Speicherverwaltung empfohlen.

WICHTIG: Bei Verwendung eines 32-Bit Windows Server-Betriebssystems mit SQL muss AWE (Addressing Windowing Extensions) aktiviert werden.

- Dual Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. zwei physikalische Prozessoren)
- 4 GB bis 10 GB RAM (1 GB für das Betriebssystem plus 1 – 2 MB pro Knoten)

WICHTIG: Die RAM-Anforderungen variieren. Multiplizieren Sie die Gesamtzahl der Geräte, die dieser Coreserver verwalten wird, mit 2 MB, für eine bessere Schätzung. 5.000 Geräte erfordern beispielsweise 6 bis 10 GB RAM.

- SQL 2005 oder SQL 2008 Enterprise oder Oracle 11g
- Drei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min
- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Ein Array für die Datenbank, RAID 0, RAID 5 oder RAID 10 oder gleichwertige/schnellere Technologie.
- Ein Array für die Datenbankprotokolle, RAID 0, RAID 1, RAID 5 oder gleichwertige/schnellere Technologie.

WICHTIG: Der Datenbankserver in dieser Konfiguration erfordert drei Laufwerkarrays auf separaten Spindeln.

- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)

Konfiguration mit mehreren Servern (5.000 bis 8.000 Geräte)

Wenn die Management Suite-Verwaltungsdomäne 5.000 bis 8.000 Geräte umfasst, empfiehlt LANDesk, die Management Suite-Komponenten auf zwei Server aufzuteilen, um eine bessere Datenbankperformance zu erzielen. Stellen Sie vor der Installation von Management Suite sicher, dass die Server die folgenden Systemanforderungen erfüllen.

Management Suite-Coreserver und Webkonsolensoftware auf einem Server

- Quad Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. vier physikalische Prozessoren)

WICHTIG: Bei Verwendung eines 32-Bit Windows Server-Betriebssystems mit SQL muss AWE (Addressing Windowing Extensions) aktiviert werden.

- Mindestens 4 GB RAM

WICHTIG: Der Management Suite-Coreserver in dieser Konfiguration erfordert zwei Laufwerkarrays auf separaten Spindeln.

- Zwei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min
- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Die Management Suite-Software sollte auf einem Array mit RAID 0, RAID 1, RAID 5 oder RAID 10 oder gleichwertiger/schnellerer Technologie installiert werden.
- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)

Coredatenbank auf einem zweiten Server

- Für den Datenbankserver wird ein 64-Bit-Betriebssystem zur Speicherverwaltung empfohlen.
- Dual Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. zwei physikalische Prozessoren)

- 6 GB bis 12 GB RAM (1 GB für das Betriebssystem plus 1 – 2 MB pro Knoten)

WICHTIG: Die RAM-Anforderungen variieren. Multiplizieren Sie die Gesamtzahl der Geräte, die dieser Coreserver verwalten wird, mit 2 MB, für eine bessere Schätzung. 8.000 Geräte erfordern beispielsweise 9 bis 16 GB RAM.

- SQL 2005 oder SQL 2008 Enterprise oder Oracle 11g
- Drei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min
- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Ein Array für die Datenbank, RAID 0, RAID 5 oder RAID 10 oder gleichwertige/schnellere Technologie.
- Ein Array für die Datenbankprotokolle, RAID 0, RAID 1, RAID 5 oder gleichwertige/schnellere Technologie.

WICHTIG: Der Datenbankserver in dieser Konfiguration erfordert drei Laufwerkarrays auf separaten Spindeln.

- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)

Konfiguration mit mehreren Servern (8.000 bis 16.000 Geräte)

Wenn die Management Suite-Verwaltungsdomäne 8.000 und mehr Geräte umfasst, empfiehlt LANDesk, die Management Suite-Komponenten auf zwei Server aufzuteilen, um in allen Bereichen eine bessere Performance zu erzielen. Stellen Sie vor der Installation von Management Suite sicher, dass die Server die folgenden Systemanforderungen erfüllen.

Management Suite-Coreserver und Webkonsolensoftware auf einem Server

- Vier physikalische Prozessoren, jeder Dual-Core oder besser
- 4 bis 8 GB RAM
- Zwei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min
- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Die Management Suite-Software sollte auf einem Array mit RAID 0, RAID 1, RAID 5 oder RAID 10 oder gleichwertiger/schnellerer Technologie installiert werden.

WICHTIG: LANDesk führt eine große Zahl von Schreibvorgängen in den folgenden Ordnern unter LDLogon durch: LDScan, VulscanResults, sdstatus, AlertQueue usw. Die Datenträger-E/A lässt sich dadurch verbessern, dass ein Laufwerk als Ordner anstatt eines Laufwerksbuchstaben bereitgestellt wird, wie z. B. LDlogon.

WICHTIG: Der Management Suite-Coreserver in dieser Konfiguration erfordert zwei Laufwerkarrays auf separaten Spindeln.

- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.

- Das Anwendungsarray sollte sich auf einem zweiten RAID-Array befinden.
- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)

Coredatenbank auf einem zweiten Server

- Für den Datenbankserver wird ein 64-Bit-Betriebssystem zur Speicherverwaltung empfohlen.

WICHTIG: Bei Verwendung eines 32-Bit Windows Server-Betriebssystems mit SQL muss AWE (Addressing Windowing Extensions) aktiviert werden.

- Quad Intel Xeon Quad Core 64-Bit-Prozessoren (d. h. vier physikalische Prozessoren)
- Mindestens 12 bis 24 GB RAM

WICHTIG: Die RAM-Anforderungen variieren. Multiplizieren Sie die Anzahl der Geräte, die dieser Coreserver verwalten wird, mit 1 bis 2 MB, für eine bessere Schätzung. 16.000 Geräte erfordern beispielsweise 17 bis 24 GB RAM.

- SQL 2005 oder SQL 2008 Enterprise oder Oracle 11g
- Drei Arrays mit 72 GB freiem Speicherplatz pro Array auf Laufwerken mit mindestens 15.000 U/min oder gleichwertiger/schnellerer Technologie
- Das Betriebssystemarray sollte RAID 1 sein oder eine gleichwertige/schnellere Technologie aufweisen.
- Ein Array für die Datenbank, RAID 0, RAID 5 oder RAID 10 oder gleichwertige/schnellere Technologie.
- Ein Array für die Datenbankprotokolle, RAID 0, RAID 1 oder RAID 5 oder gleichwertige/schnellere Technologie.
- Ein Gigabit-Netzwerkadapter (der Core und die Datenbank sollten eine Gigabit-Verbindung aufweisen)

Konfiguration mit mehreren Servern (16.000 oder mehr Geräte)

Mit den neuen Enterprise-Corefunktionen bietet LANDesk jetzt Unterstützung für Einzelcoreserver mit mehr als 16.000 Knoten. Für LANDesk Management Suite-Installationen dieser Größe und darüber hinaus empfehlen wir Ihnen, zusätzliche Unterstützung bei der Optimierung Ihrer Konfiguration von LANDesk Professional Services oder einem anerkannten Expert Solutions Provider (ESP) in Anspruch zu nehmen.

Ausführen von LANDesk Management Suite Setup

Stellen Sie vor der Installation von Management Suite sicher, dass der von Ihnen gewählte Server die zuvor in diesem Abschnitt beschriebenen Systemanforderungen erfüllt. Mit den im Folgenden beschriebenen Schritten wird Management Suite mit der standardmäßigen Microsoft SQL Express 2008-Datenbank installiert. Wenn Sie eine der anderen unterstützten Datenbanken verwenden, müssen Sie diese Datenbank installieren und konfigurieren, bevor Sie das Setupprogramm von Management Suite ausführen. Ausführliche Informationen hierzu und zur Installation von Management Suite finden Sie bei der LANDesk Benutzercommunity auf folgender Website: http://support.landesk.com.

Vor der Installation von LANDesk Management Suite 9.5 müssen sowohl der Indexdienst als auch der Windows-Suchdienst deaktiviert werden. Geschieht dies nicht, schlägt die Installation unter Umständen fehl. Weitere Informationen finden Sie in dem folgenden Artikel: http://community.landesk.com/support/docs/DOC-7245.

Stellen Sie ferner sicher, dass auf dem Server, auf dem Sie die Installation durchführen, der Microsoft Windows Server Update Service nicht installiert ist. Ist dieser Service aktiv, werden Sie Probleme bei der Anmeldung an der Konsole bekommen.

Da jede Umgebung andere Anforderungen hat, empfehlen wir Ihnen, sich bezüglich Certified LANDesk Deployment an Ihren Händler oder Expert Solution Provider (ESP) zu wenden. Wenn Sie nicht sicher sind, welcher Händler für Sie zuständig ist, gehen Sie zur folgenden Website, um einen LANDesk Inside Sales Manager zu finden, der Sie an einen Händler verweisen kann.

- http://www.landesk.com/wheretobuy/default.aspx

Weiteres erfahren Sie auf folgender Website:

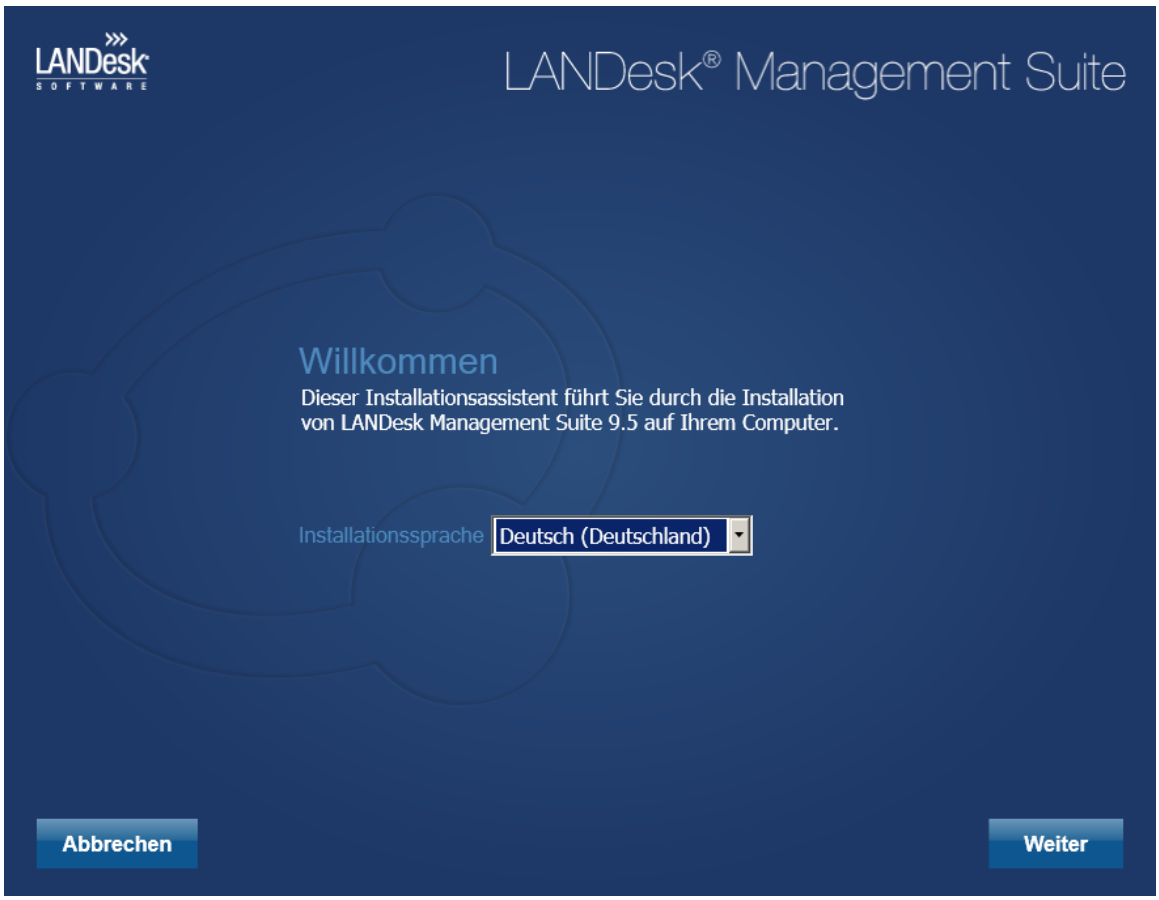
- http://www.landesk.com/SupportDownload/Support.aspx?id=3215

Beim Management Suite-Setup werden auf dem Coreserver Ports in der Windows-Firewall geöffnet. In der Regel werden diese Ports automatisch beim Management Suite-Setup und der Agentenkonfiguration konfiguriert. Wenn Sie eine andere Firewall verwenden, müssen Sie diese Ports manuell konfigurieren. Weitere Informationen zu den von Management Suite verwendeten Ports finden Sie unter folgender URL:

- Von Management Suite verwendete Ports – Vollständige Liste
  http://community.landesk.com/support/docs/DOC-1591

So installieren Sie LANDesk Management Suite

1. Starten Sie Setup.exe von Ihrem Installationsmedium.



2. Wählen Sie im Haupt-Willkommensbildschirm eine Installationssprache aus und klicken Sie dann auf **Weiter**.
3. Akzeptieren Sie die Lizenzvereinbarung und klicken Sie dann auf **Weiter**.
4. Vergewissern Sie sich, dass auf der Seite **Was möchten Sie installieren?** die Option **Coreserver** ausgewählt ist und klicken Sie anschließend auf **Weiter**.
5. Stellen Sie sicher, dass Ihr Server die Systemanforderungsprüfung laut der Seite **Voraussetzungen** besteht. Sollte er diese Voraussetzungen nicht erfüllen, installieren Sie die fehlenden Komponenten und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf der Seite **Wie soll LANDesk Ihre Datenbank konfigurieren?** auf **Neue 9.5-Datenbank konfigurieren** und klicken Sie dann auf **Weiter**.
7. Wählen Sie auf der Seite **Datenbankanwendung** die Option **SQL Express (Gebündelt)** und klicken Sie auf **Weiter**.
8. Klicken Sie auf der Seite **Wo möchten Sie installieren?** auf **Weiter**, um den Standardinstallationspfad (C:\Programme (x86)\LANDesk\ManagementSuite\) zu akzeptieren.
9. Klicken Sie auf der Seite **Installationsbereit** auf **Installieren**.
10. Wenn das Setup abgeschlossen ist, klicken Sie auf **Jetzt neu starten**.
11. Warten Sie nach dem Neustart fünf Minuten, bis alle Dienste gestartet sind.
12. Aktivieren Sie Ihren Core wie unter "Aktivieren des Coreservers" auf Seite 74 beschrieben.
13. Starten Sie die Konsole und melden Sie sich mit den Windows-Anmeldeinformationen des Benutzers an, der beim Management Suite Setup auf dem System angemeldet war. (Dieser Benutzer erhält während des Setups automatisch vollständige Administratorrechte auf der Konsole.)

Wenn Sie die Konsole starten, wird ein Assistent namens "Erste Schritte" aufgerufen, der Ihnen Hilfestellung bei der Konfiguration von Management Suite gibt. Es ist wichtig, dass Sie diese Schritte vollständig ausführen. Wenn Sie damit fertig sind, lesen Sie "Konfigurieren von Geräteagenten" auf Seite 105 und besuchen Sie die LANDesk Benutzercommunity unter http://community.landesk.com, um Näheres über die Agentenbereitstellung zu erfahren.

Einrichtung zusätzlicher Management Suite Konsolen

Die Management Suite Konsole wird automatisch auf dem Coreserver installiert. Diese Konsole sollte auf Geräten für LANDesk Administratoren installiert werden, die volle Funktionalität bzw. Zugriff auf alle Extras von Management Suite benötigen. Die Konsole wird für die Interaktion mit den verschiedenen Funktionen von Management Suite verwendet, wie beispielsweise für die Verteilung von Software, zur Remotesteuerung von verwalteten Geräten, zum Anzeigen von Inventardaten und zur Durchführung anderer Verwaltungsfunktionen.

Im gesamten Netzwerk können Konsolen für weitere Dienste und Funktionen installiert werden. (LANDesk Software berechnet keine zusätzlichen Gebühren für zusätzliche Konsolen.)

Nähere Informationen zu den unterstützten Plattformen finden Sie auf der Website der LANDesk Benutzercommunity in folgendem Dokument: http://community.landesk.com/support/docs/DOC-7478.

So installieren Sie eine zusätzliche Konsole

1. Starten Sie Autorun von Ihrem Management Suite Installationsmedium.
2. Klicken Sie auf die Schaltfläche **Remotekonsole**.
3. Klicken Sie auf **Weiter**.

4. Wenn die Voraussetzungsüberprüfung bestanden wurde, klicken Sie auf **Fortfahren**. Andernfalls müssen Sie dafür sorgen, dass die fehlenden Voraussetzungen erfüllt werden.
5. Klicken Sie auf **Setup ausführen**.
6. Folgen Sie den Installationsanweisungen.

Einrichten der Webkonsole

Die Webkonsole stellt eine Teilauswahl der Funktionen der Management Suite Konsole zur Verfügung, ergänzt durch die Vorteile eines Webbrowsers. Wenn die Webkonsole auf einem Webserver installiert ist, können ausgewählte Benutzer mit Microsoft Internet Explorer oder einem anderen unterstützten Webbrowser auf die Webkonsole zugreifen. Dieses Setup (das standardmäßig auf dem Coreserver installiert wird) gibt Benutzern Zugriff auf die Webkonsole, ohne dass eine zusätzliche Installation auf ihren lokalen PCs notwendig ist.

Standardmäßig stellt das Setupprogramm die Webkonsolendateien in den Ordner \Inetpub\wwwroot\remote.

Das Setupprogramm erstellt darüber hinaus die nachstehend aufgeführten Webkonsolen-Dateifreigaben (inklusive der erforderlichen Berechtigungen) auf Ihrem Coreserver.

Für einen fehlerfreien Betrieb benötigen Webkonsole und verwaltete Geräte die folgenden Freigaben und Berechtigungen:

- **ldmain:** Serveranwendungen (\Programme\LANDesk\ManagementSuite). Die Gruppe "Administratoren" muss über die Berechtigung "Vollzugriff" verfügen. Für Microsoft Windows 2003 benötigt die Gruppe "Netzwerkdienst" die Berechtigungen "Lesen und Ausführen", "Ordnerinhalt auflisten" sowie "Lesen".
- **ldlog:** Protokolle (\Programme\LANDesk\ManagementSuite\log).
- **ldlogon:** Verwaltete Geräteanwendungen und Agenten (\Programme\LANDesk\ManagementSuite\ldlogon). Die Gruppe "Administratoren" muss über die Berechtigung "Vollzugriff" und die Gruppe "Jeder" muss über "Lesezugriff" verfügen.
- **Skripte:** Softwareverteilungsskripte (\Programme\LANDesk\ManagementSuite\Scripts).

Wenn die Webkonsole auf einem anderen Server als dem Coreserver installiert wird, muss der angemeldete Benutzer ein Domänenadministrator sein und das Konto des Domänenadministrators muss zu einer LANDesk Benutzergruppe des Coreservers gehören. Die Coreserver und Webkonsolenserver müssen sich in derselben Domäne befinden und jeder Benutzer, der die Webkonsole benutzen soll, muss zur LANDesk Benutzergruppe auf dem Coreserver und auf den Webkonsolenservern hinzugefügt werden.

Die Management Suite 9 Webkonsole kann nicht auf einem älteren Coreserver oder einer älteren Konsolenversion ausgeführt werden. Auf einem Management Suite 9 Coreserver oder Konsolencomputer kann ausschließlich die Management Suite 9 Webkonsole ausgeführt werden. Frühere Versionen von Management Suite können nicht eingesetzt werden.

Die Webkonsole wird auf einem Microsoft Windows 2003-Server installiert, wobei Internet Information Server (IIS) standardmäßig Active Server Pages (ASP) deaktiviert. Die Active Server Pages müssen aktiviert werden, damit die Webkonsole ordnungsgemäß arbeitet.

So aktivieren Sie Active Server Pages auf Microsoft Windows 2003-Servern

1. Klicken Sie auf **Start | Verwaltung | Internetinformationsdienste (ISS)-Manager**.
2. Klicken Sie auf den <Coreservernamen>, um ihn zu erweitern.
3. Klicken Sie auf **Webdiensterweiterung**.

4. Klicken Sie auf **Active Server Pages**.
5. Klicken Sie auf **Zulassen**.
6. Schließen Sie das Fenster des Internetinformationsdienste-Managers.

Um die Installation der Webkonsole zu verifizieren, können Sie einen Webbrowser öffnen und die URL des Webservers eingeben. Standardmäßig lautet diese URL:

- http://<Webservername>/remote

Die Installation war erfolgreich, wenn der Browser zur Eingabe der Anmeldeinformationen auffordert und die Konsole geöffnet wird.

Wird die Konsole erstmalig in einem Browser gestartet, kann es bis zu 90 Sekunden dauern, bis sie angezeigt wird. Der Grund für die Verzögerung liegt darin, dass der Server einmalig Konsolencode kompilieren muss. Die Konsole wird nach dem erstmaligen Aufruf bedeutend schneller gestartet.

Wenn Ihnen beim Zugriff auf die Webkonsole die Berechtigung verweigert wird, sollten Sie sicherstellen, dass die "Integrierte Microsoft Windows-Authentifizierung" als Authentifizierungsmethode für die Website der Webkonsole aktiviert ist.

So verifizieren Sie die Authentifizierungsmethode

1. Klicken Sie auf **Start > Verwaltung > Internetinformationsdienste (ISS)-Manager**.
2. Klicken Sie auf **<Coreservername> > Websites > Standardwebsite**.
3. Klicken Sie im Dropdownmenü des Ordners **Remote** auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie im Feld **Anonymous access and authentication control** (Anonymer Zugriff und Authentifizierung) auf **Bearbeiten**.
6. Deaktivieren Sie das Kontrollkästchen **Anonymen Zugriff aktivieren**.
7. Aktivieren Sie das Kontrollkästchen **Integrierte Windows-Authentifizierung**.
8. Klicken Sie auf **OK**, um das Dialogfeld **Authentifizierungsmethoden** zu schließen.
9. Klicken Sie auf **OK**, um das Fenster **Remote Eigenschaften** zu schließen.
10. Schließen Sie das Fenster des Internetinformationsdienste-Managers.

Vergleich der Funktionen von Konsole und Webkonsole

Die folgende Tabelle gibt Aufschluss über die Merkmale und Funktionen der Management Suite Konsole und der Management Suite Webkonsole.

Merkmal oder Funktion	Konsole	Webkonsole	Hinweise
Agentenkonfiguration	Ja	Minimal	Geplante Tasks zur Agentenbereitstellung und Updatetasks sind für Webkonsolenbenutzer mit Rechten zur Agentenkonfiguration sichtbar und steuerbar.
Alarmfunktion	Ja	Nein	
Antivirus	Ja	Nein	
Spaltensatzkonfiguration	Ja	Ja	Beim Webkonsolenzugriff auf der Registerkarte

Merkmal oder Funktion	Konsole	Webkonsole	Hinweise
			"Benutzerdefinierte Spalten" unter Einstellungen.
Dienste konfigurieren	Ja	Nein	
Connection Control Manager	Ja	Minimal	Geplante Bereitstellungen können von Webkonsolenbenutzern mit Rechten für CCM eingesehen und gesteuert werden.
Benutzerdefinierte Datenformulare	Ja	Nein	
Verteilungsmethoden	Ja	Ja	Registerkarte unter "Verteilung" in der Webkonsole.
Rechtsklick auf Gerät	Ja	Ja	Stark unterschiedliches Verhalten – die einzige überlappende Funktion ist die Ausführung eines Inventarscans (auf Webkonsole "Gerät scannen")
Verzeichnis-Manager	Ja	Ja	
Display Manager	Ja	Nein	
Verteilungspakete	Ja	Ja	
Host Intrusion Prevention	Ja	Nein	
LaunchPad Link-Manager	Ja	Minimal	Geplante LaunchPad-Linkbereitstellungen können von Webkonsolenbenutzern mit Rechten zur Softwareverteilung eingesehen und gesteuert werden.
Protokolle	Ja	Nein	
Skripte verwalten	Ja	Teilweise	Über "Skripte" können vorhandene Skripte geplant und gruppiert werden.
Betriebssystem-Verteilung	Ja	Minimal	Vorhandene Skripte für die Betriebssystembereitstellung (OSD-Skripte), die bereits geplant sind, können von Webkonsolenbenutzern, die Rechte für OSD haben, über Skripte > OSD-Skripte angezeigt und gesteuert werden.
Energieverwaltung	Ja	Minimal	Geplante Energierichtlinientasks sind möglicherweise für Webkonsolenbenutzer sichtbar und steuerbar.
Versorgung (Provisioning)	Ja	Nein	
PXE-Startmenü	Ja	Nein	
Abfragefunktion	Ja	Teilweise	Die Webkonsole erlaubt den Einsatz einer Zählfunktion, die in der Windows-Konsole nicht existiert. Abfragen können in der Webkonsole nicht als Berichte angezeigt werden.
Remotesteuerung	Ja	Ja	
Berichte	Ja	Ja	Die Berichtskonsole wird in einem separaten Browserfenster gestartet.

Merkmal oder Funktion	Konsole	Webkonsole	Hinweise
Geplante Tasks	Ja	Ja	
Bereiche	Ja	Teilweise	Vorhandene Bereiche können bei einem Benutzer hinzugefügt werden, aber es können keine neuen Bereiche erstellt werden.
Sicherheits- und Patchmanagement	Ja	Minimal	Geplante Scans und Reparaturtasks können von Webkonsolenbenutzern mit Patchmanagementrechten eingesehen und gesteuert werden.
Softwarelizenzüberwachung	Ja	Teilweise	In der Webkonsole können Daten zur Produktverwendung nicht eingesehen werden, Berichte zu einzelnen Produkten und zur Gruppencompliance stehen nicht zur Verfügung, und Produkte können nicht ignoriert oder gruppiert werden.
Erkennung nicht verwalteter Geräte	Ja	Minimal	Geplante Scans zur Erkennung von nicht verwalteten Geräten können von Webkonsolenbenutzern mit UDD-Rechten eingesehen und gesteuert werden.
Benutzer	Ja	Nein	
Windows CE-Agentenkonfiguration	Ja	Nein	
Windows CE CAB Creator	Ja	Nein	

Aktivieren des Coreservers

LANDesk Software, Inc. verwendet einen zentralen Lizenzserver, der Sie bei der Verwaltung der Produkt- und Knotenlizenzen Ihres Coreservers unterstützt. Um LANDesk Produkte verwenden zu können, müssen Sie von LANDesk einen Benutzernamen und ein Kennwort beziehen, der/das den Coreserver mit einem autorisierten Zertifikat aktiviert. Die Aktivierung muss auf jedem Coreserver durchgeführt werden, um die LANDesk Produkte auf dem betreffenden Server verwenden zu können. Sie können jeden Coreserver entweder automatisch über das Internet oder manuell per E-Mail aktivieren. Falls Sie die Hardwarekonfiguration des Coreservers erheblich ändern, müssen Sie den Coreserver u. U. reaktivieren.

Die Aktivierungskomponente des jeweiligen Coreservers generiert in regelmäßigen Abständen Daten in Bezug auf:

- Die genaue Anzahl von Knoten, die Sie verbrauchen
- Die nicht persönliche verschlüsselte Hardwarekonfiguration
- Die spezifischen LANDesk Softwareprogramme, die Sie verwenden ("Daten zur Knotenzahl")

Dies sind die einzigen Daten, die von der Aktivierung erfasst oder generiert werden. Der Code für den Hardwareschlüssel wird auf dem Coreserver unter Verwendung nicht persönlicher Faktoren für die Hardwarekonfiguration (beispielsweise die Größe der Festplatte, die Verarbeitungsgeschwindigkeit des Computers etc.) generiert. Der Code für den Hardwareschlüssel wird verschlüsselt an LANDesk gesendet, während sich der für die Verschlüsselung verwendete private Schlüssel nur auf dem Coreserver befindet. Der Code für den Hardwareschlüssel wird dann von LANDesk zur Erstellung eines Teils des autorisierten Zertifikats verwendet.

Aktivieren Sie den Coreserver, nachdem Sie ihn installiert haben, mithilfe des Coreserver-Aktivierungsprogramms (**Start > Programme > LANDesk > Coreserver aktivieren**). Sie können den Coreserver entweder mit einem LANDesk Konto, das mit den von Ihnen erworbenen Lizenzen verknüpft ist, oder mit einer 45 Tage gültigen Evaluierungslizenz aktivieren. Die 45 Tage gültige Probelizenz deckt 100 Knoten ab. Der Evaluierungszeitraum von 45 Tagen beginnt mit der erstmaligen Aktivierung eines Produkts auf dem Coreserver. Wenn Sie zu einem späteren Zeitpunkt während der 45-tägigen Zeitspanne andere LANDesk Produkte zu Testzwecken auf dem Coreserver installieren, verlängert sich die ursprüngliche 45-tägige Evaluierungsperiode dadurch nicht . Alle LANDesk Produkte auf einem Coreserver, teilen sich eine Evaluierungslizenz und den gemeinsamen 45-tägigen Evaluierungszeitraum.

Mithilfe des Autorun-Programms der Installations-CD können Sie zusätzliche LANDesk Produkte unter Ihrer 45-tägigen Evaluierungslizenz installieren. Installieren Sie vom Autorun-Fenster aus die gewünschten Produkte und wählen Sie während des Setups die Option **Ändern** aus. Anschließend können Sie dann LANDesk Produkte auf Ihrem Coreserver hinzufügen oder entfernen.

Sie können die 45-tägige Probelizenz jederzeit in eine Volllizenz konvertieren, indem Sie das Coreserver-Aktivierungstool ausführen und Ihren LANDesk Benutzernamen und Ihr Kennwort eingeben.

Es gibt zwei verschiedene Lizenztypen: Clientlizenz und Serverlizenz. Immer, wenn Sie Management Suite Agenten auf einem Serverbetriebssystem wie Windows 2000 Server oder Windows 2003 Server installieren, verbrauchen Sie eine Management Suite Lizenz pro Server. Rollup-Coreserver müssen nicht aktiviert werden.

Immer, wenn die Aktivierungssoftware auf einem Coreserver die Daten zur Knotenzahl generiert, müssen Sie diese Daten entweder automatisch über das Internet oder manuell per E-Mail an LANDesk weiterleiten. Wenn Sie innerhalb einer Verzugsfrist von 30 Tagen – nach dem ersten Versuch, die Knotenzahl in Erfahrung zu bringen – keine Knotendaten bereitstellen, bleibt der Coreserver so lange deaktiviert, bis LANDesk die entsprechenden Knotenzahldaten von Ihnen erhalten hat. Sobald Sie die Daten zur Knotenzahl gesendet haben, erhalten Sie von LANDesk ein autorisiertes Zertifikat, mit dem sich der normale Betriebsmodus des Coreservers wieder aktivieren lässt.

Öffnen Sie nach der Aktivierung eines Coreservers in der Management Suite Konsole das Dialogfeld **Konfigurieren > Produktlizenzierung**, um die Produkte und die Zahl der autorisierten Knoten anzuzeigen, die für das Konto, bei dem der Coreserver authentifiziert wird, erworben wurden. Sie können in diesem Dialogfeld auch überprüfen, an welchem Datum der Coreserver die Knotenzahldaten mit dem zentralen Lizenzserver abgleichen wird. Der Coreserver schränkt Sie nicht auf die Anzahl der autorisierten Knoten ein, die Sie erworben haben.

Informationen zum Coreserver-Aktivierungsprogramm

Verwenden Sie das Coreserver-Aktivierungsprogramm für folgende Aufgaben:

- Erstmalige Aktivierung eines neuen Servers
- Aktualisierung eines vorhandenen Coreservers oder Konvertierung einer Probelizenz in eine Volllizenz
- Aktivierung eines neuen Servers mit einer 45 Tage gültigen Probelizenz

Starten Sie das Programm, indem Sie auf **Start > Alle Programme > LANDesk > Coreserver-Aktivierung** klicken. Wenn Ihr Coreserver nicht mit dem Internet verbunden ist, lesen Sie die Informationen unter "Manuelles Aktivieren eines Cores oder Überprüfen der Knotenzahldaten" auf Seite 77.

Jeder Coreserver benötigt ein eindeutiges Autorisierungszertifikat. Das Autorisierungszertifikat darf nicht von mehreren Coreservern gemeinsam benutzt werden; mehrere Coreserver können jedoch Knotenzahlen beim selben LANDesk Konto verifizieren lassen.

Der Coreserver hinterlegt in regelmäßigen Abständen zu verifizierende Knotenzahldaten in der Datei "\Programme\LANDesk\Authorization Files\LANDesk.usage". Diese Datei wird in regelmäßigen Abständen an den LANDesk Lizenzserver gesendet. Die Datei wird im XML-Format erstellt und digital signiert und verschlüsselt. Jegliche Änderungen, die manuell an dieser Datei vorgenommen werden, machen ihren Inhalt und den nächsten Nutzungsbericht an den LANDesk Lizenzserver ungültig.

Der Core kommuniziert mit dem LANDesk Lizenzserver über HTTP. Wenn Sie einen Proxy-Server verwenden, klicken Sie auf die Registerkarte **Proxy** und geben die erforderlichen Proxy-Informationen ein. Wenn Ihr Core mit dem Internet verbunden ist, wird die Kommunikationsverbindung mit dem Lizenzserver automatisch, d.h. ohne Ihr Eingreifen, hergestellt.

Beachten Sie, dass das Coreserver-Aktivierungsprogramm keine DFÜ-Verbindungen automatisch startet. Wenn Sie eine DFÜ-Verbindung jedoch manuell starten und dann das Aktivierungsprogramm ausführen, kann das Programm die Daten zur Nutzung auch über eine DFÜ-Verbindung weiterleiten.

Wenn Ihr Coreserver nicht mit dem Internet verbunden ist, können Sie die Knotenzahldaten auch manuell überprüfen und weiterleiten. Lesen Sie hierzu die Ausführungen weiter unten in diesem Abschnitt.

Aktivieren eines Servers mit einem LANDesk Konto

Bevor Sie einen neuen Server mit einer Volllizenz aktivieren können, müssen Sie ein LANDesk Konto eingerichtet haben, das Ihnen eine Lizenz für die von Ihnen erworbenen LANDesk Produkte und die Anzahl der Knoten erteilt hat. Sie benötigen die Kontoinformationen (Name der Kontaktperson und Kennwort), um Ihren Server zu aktivieren. Wenn Ihnen diese Informationen nicht vorliegen, wenden Sie sich an den für Sie zuständigen LANDesk Vertriebsbeauftragten.

So aktivieren Sie einen Server

1. Klicken Sie auf **Start > Programme > LANDesk > Coreserver aktivieren**.
2. Klicken Sie auf **Die Lizenz dieses Servers mithilfe Ihres LANDesk Kontaktnamens und Kennwortes aktivieren.**
3. Geben Sie den Namen der **Kontaktperson** und das **Kennwort** ein, den/das der Core verwenden soll.
4. Klicken Sie auf **Aktivieren**.

Aktivieren eines Servers mit einer Probelizenz

Die 45 Tage gültige Probelizenz aktiviert Ihren Server auf dem LANDesk Lizenzserver. Nach Ablauf der 45-tägigen Evaluierungsperiode können Sie sich nicht mehr beim Coreserver anmelden; der Coreserver nimmt dann auch keine Inventarscans mehr entgegen. Ihre in der Software oder Datenbank vorhandenen Daten gehen jedoch nicht verloren. Während oder nach Verwendung der 45-tägigen Probelizenz können Sie das Coreserver-Aktivierungstool erneut ausführen und Ihre Probelizenz in eine Vollaktivierung konvertieren, die mit einem LANDesk Konto arbeitet. Wenn die Probelizenz abgelaufen ist, wird mit der Konvertierung in eine Volllizenz der Core reaktiviert.

So aktivieren Sie eine 45-tägige Probelizenz

1. Klicken Sie auf **Start > Alle Programme > LANDesk > Coreserver-Aktivierung.**
2. Klicken Sie auf **Core für eine 45-tägige Testzeit aktivieren**.
3. Klicken Sie auf **Aktivieren**.

Aktualisieren eines vorhandenen Kontos

Die Aktualisierungsoption sendet Nutzungsdaten an den LANDesk Lizenzserver. Die Nutzungsdaten werden automatisch gesendet, wenn Ihr System über eine Internet-Verbindung verfügt. Es sollte sich daher im Allgemeinen für Sie nicht als notwendig erweisen, mit dieser Option Daten zur Verifizierung der Knotenzahl zu senden. Sie können diese Option auch verwenden, um das LANDesk Konto zu ändern, dem der Coreserver angehört. Zudem können Sie mit dieser Option einen Coreserver von einer Probelizenz in eine Volllizenz konvertieren.

So aktualisieren Sie ein vorhandenes Konto

1. Klicken Sie auf **Start > Alle Programme > LANDesk > Coreserver-Aktivierung.**
2. Klicken Sie auf **Aktualisieren Sie die Lizenz dieses Coreservers mithilfe Ihres LANDesk Kontaktnamens und Kennworts**.
3. Geben Sie den Namen der **Kontaktperson** und das **Kennwort** ein, den/das der Core verwenden soll. Wenn Sie einen Namen oder ein Kennwort eingeben, das sich von dem für die ursprüngliche Aktivierung des Coreservers verwendeten Namen oder Kennwort unterscheidet, wird der Core hiermit dem neuen Konto zugeordnet.
4. Klicken Sie auf **Aktivieren**.

Manuelles Aktivieren eines Cores oder Überprüfen der Knotenzahldaten

Wenn der Coreserver nicht mit dem Internet verbunden ist, kann das Coreserver-Aktivierungsprogramm keine Informationen bzgl. der Knotenzahl senden. In diesem Fall erhalten Sie eine Meldung, in der Sie aufgefordert werden, Verifizierungsdaten zur Aktivierung und zur Knotenzahl manuell per E-Mail zu senden. Die E-Mail-Aktivierung ist ein unkompliziertes und schnelles Verfahren. Wenn die Aufforderung zur manuellen Aktivierung auf dem Core angezeigt wird, oder wenn Sie das Coreserver-Aktivierungsprogramm verwenden und die manuelle Aktivierungsmeldung angezeigt wird, führen Sie folgende Schritte aus:

So aktivieren Sie einen Core manuell oder veranlassen eine manuelle Überprüfung der Knotenzahldaten

1. Wenn der Coreserver Sie auffordert, die Knotenzahldaten manuell zu überprüfen, erstellt er eine Datei mit dem Namen {languagecode}-activate.{datestring}.txt im Ordner "\Programme\LANDesk\Authorization Files". Fügen Sie diese Datei einer E-Mail-Nachricht bei und senden Sie sie an licensing@landesk.com. Betreff und Nachrichtentext können frei gewählt werden.
2. LANDesk verarbeitet die beigefügte Datei und schickt eine Antwort an die E-Mail-Adresse, von der aus Sie die Nachricht gesendet hatten. Die LANDesk Nachricht enthält Anweisungen und eine neue Autorisierungsdatei.
3. Speichern Sie die beigefügte Autorisierungsdatei im Ordner "\Programme\LANDesk\Authorization Files". Die Datei wird daraufhin sofort vom Coreserver verarbeitet und ihr Aktivierungsstatus aktualisiert.

Wenn die manuelle Aktivierung misslingt oder der Core die beigefügte Aktivierungsdatei nicht verarbeiten kann, wird die von Ihnen kopierte Autorisierungsdatei unter Verwendung der Erweiterung ".rejected" umbenannt. Zusätzlich hierzu protokolliert das Aktivierungsprogramm unter Angabe weiterer Details ein Ereignis im Anwendungsprotokoll der Windows-Ereignisanzeige.

Konfigurieren von COM+-Serveranmeldeinformationen

Wenn Sie einen Webkonsolenserver verwenden möchten, der sich nicht auf dem Core befindet, oder wenn Sie Domänengruppen innerhalb der LANDesk Management Suite-Gruppe auf dem Coreserver verwenden möchten, müssen Sie zusätzliche Schritte zum Konfigurieren des Servers ausführen, damit die Management Suite Authentifizierung ordnungsgemäß arbeitet. Remote-Webkonsolenserver müssen Datenbankverbindungsinformationen und Benutzerinformationen aus dem Coreserver abrufen; da Remote-Webkonsolenserver jedoch per "Identitätswechsel" angenommene Web-Anmeldeinformationen auf IIS (Internet Information Services) verwenden, können sie nicht direkt mit dem Coreserver kommunizieren.

Webkonsolenserver und Coreserver lösen dieses Problem, indem sie eine COM+-Anwendung verwenden, um über HTTPS zu kommunizieren; auf diese Weise kann der Webkonsolenserver Coreserver-Datenbankinformationen und -Benutzerinformationen abrufen. Sie müssen diese COM+-Anwendung auf dem Webkonsolenserver für die Verwendung eines Kontos konfigurieren, das über die erforderlichen Rechte verfügt, beispielsweise das Domänenadministratorkonto. Das von Ihnen bereitgestellte Konto muss sich in der LANDesk Management Suite-Gruppe auf dem Coreserver befinden (auf diese Weise erhält es Zugriff auf die Datenbankverbindungsinformationen des Coreservers) und muss Rechte zum Aufzählen von Windows-Domänenmitgliedern besitzen.

Wenn Sie Domänengruppen in der LANDesk Management Suite-Gruppe des Coreservers verwenden, muss Management Suite ebenfalls in der Lage sein, Windows-Domänenmitglieder aufzuzählen. In diesem Fall müssen Sie außerdem ein Konto für die LANDesk1 COM+-Anwendung des Coreservers bereitstellen.

So konfigurieren Sie die LANDesk1 COM+-Anwendung auf einem Coreserver oder Remote-Webkonsolenserver

1. Navigieren Sie zu dem Webserver oder Coreserver, den Sie konfigurieren möchten.
2. Öffnen Sie in der Windows-Systemsteuerung die "Verwaltung" und anschließend **Komponentendienste**.
3. Klicken Sie auf **Komponentendienste > Computer > Arbeitsplatz > COM+-Anwendungen**.
4. Klicken Sie mit der rechten Maustaste auf die **LANDesk1** COM+-Anwendung und wählen Sie dann **Eigenschaften**.
5. Geben Sie auf der Registerkarte **Identität** die Anmeldeinformationen ein, die Sie verwenden möchten.
6. Klicken Sie auf **OK**.

Unterstützte Plattformen und Funktionen

Nähere Informationen zu den von Management Suite unterstützten Betriebssystemversionen und Sprachen (für Coreserver, verwaltete Geräte sowie LANDesk Extras und Funktionen) finden Sie in den folgenden Dokumenten der LANDesk Benutzercommunity:

- Supported Platforms and Compatibility Matrix for LANDesk Management Suite
- Supported Client Languages for LANDesk Management Suite

Von Management Suite verwendete Ports

Wenn Management Suite in einer Umgebung mit Firewalls (oder Routern, die den Netzwerkverkehr filtern) eingesetzt wird, muss angegeben werden, welche Ports an den Firewalls geöffnet werden müssen.

Die folgenden Dokumente auf der Website der LANDesk Benutzercommunity geben Aufschluss über die Ports, die von Management Suite auf Ihrem Coreserver und auf den verwalteten Geräten verwendet werden.

- Von Management Suite verwendete Ports – Vollständige Liste http://community.landesk.com/support/docs/DOC-1591
- Portarchitektur-Diagramm http://community.landesk.com/support/docs/DOC-8092

WICHTIG: In der Regel werden diese Ports automatisch beim Setup von LANDesk Management Suite und bei der Agentenkonfiguration in der Windows-Firewall konfiguriert. Wenn Sie ein anderes Firewallprodukt verwenden, müssen Sie diese Ports manuell konfigurieren.

Verbesserungen bei der Coreserver-Sicherheit

LANDesk möchte sicherstellen, dass Sie größtes Vertrauen in die Sicherheit – nicht nur Ihrer verwalteten Geräte und geschützten Endbenutzergeräte – sondern auch in die Sicherheit Ihrer LANDesk Coreserver, Rollup-Cores und zusätzlichen Konsolen haben.

Mit der neuesten Version haben wir mehrere entscheidende Vorkehrungen getroffen, die zum Erreichen dieses Ziels beitragen.

Mit Version 9.5 eingeführte Coreserver-Sicherheitsfunktionen

LANDesk® Management Suite Version 9.5 hat mehrere intelligente Verbesserungen im Hinblick auf die Sicherheit des LANDesk Coreserver zu bieten. Diese Verbesserungen zielen darauf ab, LANDesk Systemadministratoren darin zu unterstützen, ihre Coreserver im Netzwerk umfassender abzusichern und zu schützen – vor Angriffen durch Schadsoftware, unberechtigtem Zugriff und anderen gängigen Sicherheitsrisiken.

Die Verbesserungen der Coreserver-Sicherheit sind nicht auf ein bestimmtes Extra, einen bestimmten Dienst oder eine bestimmte Schnittstelle in der LANDesk Konsole beschränkt; sie verteilen sich vielmehr auf verschiedene Stellen innerhalb des Produkts. Damit Sie diese wichtigen Upgrades der Coreserver-Sicherheit schnell und einfach verstehen, überwachen und gegebenenfalls diesbezüglich nachfassen können, sind sie hier in einem einzigen Hilfethema zusammengeführt und beschrieben.

In diesem Thema wird beschrieben, an welchen Stellen diese Verbesserungen der Sicherheit vorgenommen wurden. Sie werden entweder hier erläutert oder es wird mit einem Link auf die entsprechende Funktion verwiesen, unter Sie weitere Einzelheiten finden.

Die folgenden Funktionen und Merkmale wurden zur Verstärkung der Sicherheit des Coreservers hinzugefügt und/oder erweitert.

- "Beschränkung des Zugriffs auf die Freigabe "LDMAIN"" auf Seite 80
- "Sicherheitsverbesserungen bei den Webdiensten und bei der Webkonsole" auf Seite 81
- "Deaktivierung des remoten Zugriffs auf die Registrierung" auf Seite 82
- "Updates für Open SSL" auf Seite 82

- "Verbesserungen bei der verschlüsselten Datenbank" auf Seite 83
- "Zur Verbesserung der Coreserver-Sicherheit entfernte Funktionen / Elemente" auf Seite 83

Beschränkung des Zugriffs auf die Freigabe "LDMAIN"

Die LDMAIN-Freigabe ist gesperrt. Der Grund hierfür ist, dass allgemeinen LANDesk Benutzern der Zugriff auf diesen Ordner verwehrt werden soll, da sie darin enthaltene kritische Dateien (z. B. benutzerdefinierte Skriptdateien) ändern könnten.

HINWEIS: Benutzerdefinierte Skripts wurden verschoben
Um einen nicht autorisierten Zugriff zu verhindern, wurden die benutzerdefinierten Skriptdateien in die Coredatenbank verschoben.

Die LDMAIN-Freigabe erforderte ein höheres Maß an Sicherheit. Zu diesem Zweck wurden die folgenden Änderungen vorgenommen:

LDMAIN wurde aus dem Ordner:

```
C:\Programme (x86)\LANDesk\ManagementSuite (d. h. der ehemaligen LDMAIN-Freigabe)
```

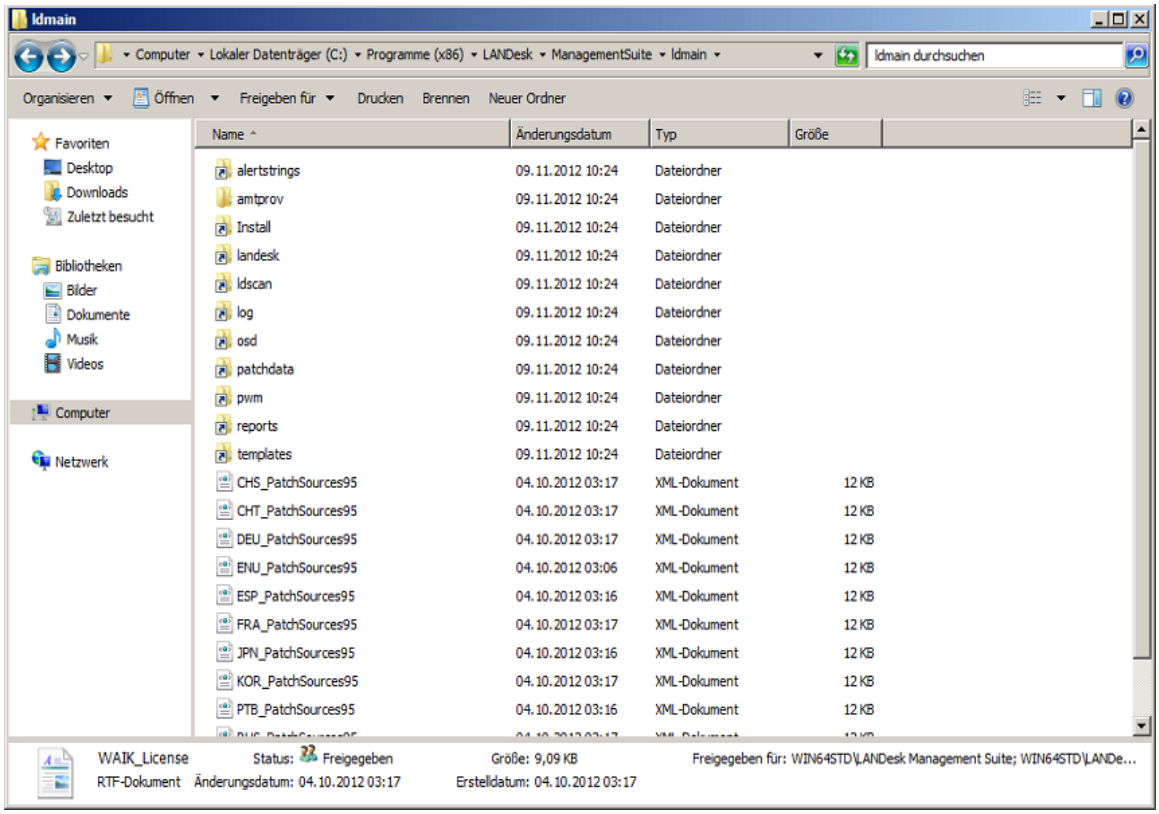
in einen neuen separaten Unterordner mit folgendem Namen verschoben:

```
C:\Programme (x86)\LANDesk\ManagementSuite\ldmain (d. h. in einen jetzt eindeutig identifizierbaren Ordner)
```

Die LDMAIN-Freigabe enthält jetzt weniger Dateien und Ordner. Administratoren (mit entsprechenden Rechten) können nach wie vor Programmdateien nach Belieben in die Freigabe "LDMAIN" kopieren, diese weist jedoch eine viel klarere, eingeschränkte und zielgerichtete Struktur auf.

WICHTIG: Die rollenbasierten administrativen Rechte wurden beschränkt
Zusätzlich wurden die rollenbasierten administrativen Rechte beschränkt, um den Zugriff auf die LDMAIN-Freigabe zu unterbinden. Die Gruppe LANDesk Management Suite besitzt für diesen Ordner keine Rechte des Typs **Vollzugriff** oder **Ändern** mehr. Mitglieder dieser Gruppe können nach wie vor Skripts lesen und ausführen usw. Der Lese-oder Schreibzugriff auf Dateien in der LDMAIN-Freigabe ist jedoch den Mitgliedern der Gruppe "LANDesk Administratoren" vorbehalten.

Der LDMAIN-Ordner enthält mehrere Unterordner, bei denen es sich um einfache Verknüpfungen oder Zeiger im Dateisystem handelt, die auf den eigentlichen Ordner unterhalb des Ordners \LANDesk\ManagementSuite\ldmain verweisen. Diese Verknüpfungsordner sind durch ein Pfeil-Overlay gekennzeichnet wie nachstehend gezeigt:



Sicherheitsverbesserungen bei den Webdiensten und bei der Webkonsole

Zur Erhöhung der Sicherheit Ihres LANDesk Coreservers wurden die folgenden Änderungen für die Webkonsole und die Webdienste vorgenommen.

- Die Website-Sicherheit wurde auf der Basis von Penetrationstests (z. B. im Hinblick auf Pfadüberschreitung, Cross-Site Scripting und andere bekannte Webanfälligkeiten) aktualisiert.
- Die Webkonsole wurde auf NET 4.0 aktualisiert.
- Die Sicherheit der Webkonsole wurde gründlich getestet und verifiziert.
- Nicht verwendete Berichtsseiten für die Webkonsole wurden entfernt.

HINWEIS: Weitere Einzelheiten zu spezifischen Änderungen bei der Webkonsole und den Webdiensten
Nähere Einzelheiten zu Verbesserungen der Sicherheit bei der Webkonsole und den Webdiensten finden Sie in der Benutzercommunity im entsprechenden Dokument zu bewährten Methoden (Best Known Methods, BKM).

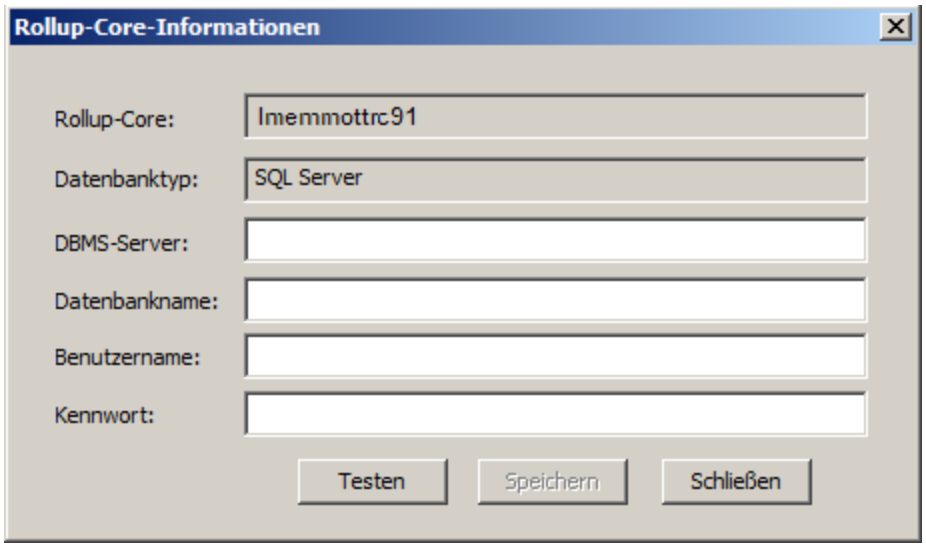
Deaktivierung des remoten Zugriffs auf die Registrierung

Der remote Zugriff auf die Registrierung beim Coreserver wurde beseitigt. Erreicht wurde dies durch Entfernen der Lese-/Schreibrechte von sämtlichen rollenbasierten administrativen LANDesk Gruppen. Sicherheitsrechte wurden von der Gruppe LANDesk Management Suite in den folgenden Registrierungsschlüssel entfernt:

```
HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
```

Anstelle eines remoten Lesens der Registrierungsdatei verwendet die Remotesteuerungskonsole jetzt sichere Web Services. Diese Änderungen sollten für den LANDesk Benutzer transparent sein.

Zusätzlich wurde die Benutzeroberfläche für DBRollup.exe aktualisiert Der Administrator muss nun die Datenbankkonfigurationsinformationen eingeben. Dies eliminiert die remoten Aufrufe der Registrierung zwischen dem Coreserver und dem Rollup-Core wie nachstehend gezeigt:



Updates für Open SSL

Tatsache ist, dass Open SSL im Zuge seiner Weiterentwicklung sicherer geworden ist. Der LANDesk Support bietet Ihnen die neuste aktualisierte Version von Open SSL.

Open SSL liegt jetzt in der Version 1.0.1c vor. Diese Version von Open SSL hat mehrere bekannte Anfälligkeiten behoben.

Die neuste Version von Open SSL finden Sie auf der Website der LANDesk Benutzercommunity:

LANDesk Benutzercommunity – Startseite

HINWEIS: Rückwärtskompatibilität für Open SSL ist gewährleistet
LANDesk hat dafür gesorgt, dass die Rückwärtskompatibilität für Open SSL gewährleistet ist, indem nach wie vor dieselben Algorithmen verwendet werden.

Verbesserungen bei der verschlüsselten Datenbank

Die Spalte CONNECTINFO in der METASYSTEMS-Tabelle ist verschlüsselt, sodass die Benutzer diese Informationen jetzt NICHT MEHR lesen können.

Zur Verbesserung der Coreserver-Sicherheit entfernte Funktionen / Elemente

Die folgenden Extras, Funktionen und Komponenten wurde aus dem Produkt LANDesk Management Suite Version 9.5 entfernt, da sie nicht länger verwendet oder unterstützt werden (bzw. um die Sicherheit der Produktsuite insgesamt durch eine Reduzierung der verknüpften Dienste zu erhöhen).

Mit anderen Worten, die folgenden Funktionen sind in Management Suite bzw. Security Suite9.5 NICHT mehr enthalten und sollten NICHT als funktionstüchtige oder unterstützte Funktionen angesehen werden.

- Off-Core-Inventardienst
- Off-Core-Webkonsole
- Handheld Manager
- NetWare-Agenteninstallation
- LinuxPE
- NetWare-Serverbereitstellung
- Veralteter Dateireplikator aus einschlägigen Dienstprogrammen
- Application Healing
- LANDesk Profile Migration

Verwandte Themen

Weitere Einzelheiten zu den in LANDesk Management Suite Version 9.5 entfernten Extras und Funktionen finden Sie auf der Benutzercommunity-Website des LANDesk Supports:

LANDesk Benutzercommunity – Startseite

Konfigurieren von Corediensten

Konfigurieren von Diensten

Viele der wichtigsten und grundlegenden Funktionen, die von LANDesk Komponenten bereitgestellt werden, wie beispielsweise der Inventarserver und Scheduler-Dienst, können und sollten von Ihnen angepasst werden, um das Leistungspotenzial Ihrer Netzwerkumgebung zu optimieren. Verwenden Sie hierfür das Applet LANDesk**Softwaredienste konfigurieren**, das Sie von der Programmgruppe **LANDesk** im Startmenü ausführen können. (Oder klicken Sie von der Managementkonsole aus auf **Konfigurieren > Dienste**.)

HINWEIS: Dienste können nur von LANDesk Administratoren konfiguriert werden.
Nur Benutzer mit dem LANDesk Administratorrecht können Diensteinstellungen ändern. Die Option **Dienste konfigurieren** steht zudem nur in der Hauptkonsole zur Verfügung, nicht in einer der zusätzlichen Konsolen, die Sie ggf. eingerichtet haben.

Dieses Thema befasst sich mit folgenden Punkten:

- "Auswählen eines Coreservers und einer Datenbank" auf Seite 84
- "Konfigurieren des Inventardienstes" auf Seite 85
- "Auflösen doppelter Gerätedatensätze in der Datenbank" auf Seite 88
- "Konfigurieren des Scheduler-Dienstes" auf Seite 89
- "Konfigurieren des Dienstes für benutzerdefinierte Tasks" auf Seite 92
- "Konfigurieren des Multicast-Dienstes" auf Seite 93
- "Konfigurieren des Dienstes für die Betriebssystembereitstellung" auf Seite 93
- "Konfigurieren des BMC-Kennworts" auf Seite 95
- "Konfigurieren der Anmeldeinformationen für die Betriebssystem-Virtualisierung" auf Seite 96

Auswählen eines Coreservers und einer Datenbank

Geben Sie vor dem Konfigurieren des Dienstes auf der Registerkarte **Allgemein** den Coreserver und die Datenbank an, für die Sie den Dienst konfigurieren möchten.

HINWEIS: Wenn Sie die Konfiguration eines Dienstes für einen Coreserver und eine Datenbank ändern, werden diese Änderungen erst übernommen, wenn Sie den Dienst auf dem betreffenden Coreserver neu starten.

Informationen zur Registerkarte "Allgemein"

Wählen Sie auf dieser Registerkarte den Coreserver und die Datenbank aus, für die Sie einen bestimmten Dienst konfigurieren möchten. Wählen Sie dann eine beliebige Registerkarte "Dienst" aus und definieren Sie die Einstellungen für den betreffenden Dienst.

Mit den Benutzeranmeldeinformationen für die Berichtsdatenbank können Sie bei Verwendung des Extras "Berichte" ein anderes Benutzerkonto zum Herstellen einer Verbindung zur Datenbank verwenden. Sie können beispielsweise ein Benutzerkonto für die Datenbank erstellen, das ausschließlich Leserechte besitzt, so dass die Benutzer des Extras "Berichte" Inhalte der Datenbank zwar lesen aber nicht ändern können.

- **Servername:** Zeigt den Namen des Coreservers an, mit dem Sie gegenwärtig verbunden sind.
- **Server:** Hier können Sie den Namen eines anderen Coreservers und dessen Datenbankverzeichnis eingeben.
- **Datenbank:** Hier können Sie den Namen der Coredatenbank eingeben.
- **Benutzername:** Identifiziert einen Benutzer mit Anmeldeinformationen zur Authentifizierung gegenüber der Coredatenbank (während des Setup festgelegt).
- **Kennwort:** Identifiziert das Benutzerkennwort, das für den Zugriff auf die Coredatenbank erforderlich ist (während des Setup festgelegt).
- **Dies ist eine Oracle-Datenbank:** Gibt an, dass die oben festgelegte Datenbank eine Oracle-Datenbank ist.
- **Berichtsdatenbankbenutzer:** Geben Sie den Benutzernamen und das Kennwort für das Konto ein, über das mit dem Extra "Berichte" auf die Datenbank zugegriffen wird. Dieses Konto muss bereits mit spezifischen Zugriffsrechten für die Datenbank erstellt worden sein.
- **Webkonsoleneinstellungen:** Zeigt den Name des Servers bzw. IP-Adresse an, auf dem bzw. der die Webkonsole ausgeführt werden kann. Wenn Sie von einem anderen Gerät aus auf die Webkonsole zugreifen möchten, geben Sie diesen Namen bzw. diese Adresse, gefolgt von "/remote" in einem Webbrowser ein.
- **Einstellungen aktualisieren:** Stellt die Einstellungen wieder her, die beim Öffnen des Dialogfelds vorhanden waren.

Bei der Angabe von Benutzernamen und Kennwörtern für eine Datenbank dürfen Benutzername und Kennwort kein Apostroph ('), Semikolon (;) oder Gleichheitszeichen (=) enthalten.

Konfigurieren des Inventardienstes

Konfigurieren Sie auf der Registerkarte **Inventar** den Inventardienst für den Coreserver und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Wenn Sie den Inventardienst auf einem geclusterten Core neu starten müssen, so muss dies über den Windows Service Control Manager geschehen. Der Inventardienst auf einem geclusterten Core kann nicht über die Schaltfläche **Neu starten** für Dienste auf der Registerkarte **Inventar** der LANDesk Softwaredienste neu gestartet werden.

Informationen zur Registerkarte "Inventar"

Definieren Sie mithilfe dieser Registerkarte die folgenden Inventaroptionen:

- **Servername:** Zeigt den Namen des Coreservers an, mit dem Sie gegenwärtig verbunden sind.
- **Statistik protokollieren:** Legt ein Protokoll mit den Aktionen der Coredatenbank und mit Statistiken an. Sie können die Protokolldaten im Protokoll der Anwendung "Windows-Ereignisanzeige" anzeigen.
- **Verschlüsselter Datentransport:** Ermöglicht es dem Inventarscanner, Daten zum Geräteinventar als verschlüsselte Daten über SSL zurück an den Coreserver zu senden.
- **Server inventarisieren um:** Gibt die Uhrzeit für die Durchführung des Coreserverscans an.
- **Wartung durchführen um:** Gibt die Uhrzeit für die Standardwartung der Coredatenbank an.
- **Tage, die Inventarscans gespeichert bleiben:** Legt fest, nach wie vielen Tagen die Daten des Inventarscans gelöscht werden.

- **Anmeldungen für "Primärer Eigentümer":** Legt fest, wie oft der Inventarscanner Anmeldungen verfolgt, um den primären Eigentümer eines Geräts zu bestimmen. Der primäre Eigentümer ist der Benutzer, der sich innerhalb dieser vorgegebenen Anzahl von Anmeldungen am häufigsten angemeldet hat. Der Standardwert ist 5 und Mindest- bzw. Höchstwerte sind 1 bzw. 16. Wenn alle Anmeldenamen unterschiedlich sind, wird der letzte Benutzer, der sich anmeldet, als primärer Eigentümer betrachtet. Ein Gerät kann nur jeweils mit einem primären Eigentümer verknüpft sein. Die Anmeldedaten des primären Eigentümers umfassen den voll qualifizierten Namen des Benutzers entweder im ADS-, NDS-, Domänennamen- oder im lokalen Namensformat (in dieser Reihenfolge) und das Datum der letzten Anmeldung.
- **Erweiterte Einstellungen:** Öffnet das Dialogfeld **Erweiterte Einstellungen**. Hier können Sie erweiterte inventarbezogene Einstellungen ändern. Beim Klicken auf die einzelnen Elemente werden Hilfetexte am unteren Rand des Dialogfelds eingeblendet, die die jeweilige Option beschreiben. Die Standardwerte sind für die meisten Installationen ausreichend. Um eine Einstellung zu ändern, klicken Sie auf die Einstellung, ändern Sie den **Wert** und klicken Sie dann auf **Festlegen**. Starten Sie nach Abschluss des Vorgangs den Inventardienst neu:
- **Unbekannte Elemente:** Öffnet das Dialogfeld **Unbekannte Inventarelemente**, in dem sämtliche Objekts aufgeführt sind, die bei Scans erkannt, aber nicht bereits in der Datenbank vorgefunden wurden. Diese Option gibt Ihnen die Möglichkeit, zu steuern, welche Elemente zur Datenbank hinzugefügt werden. Auf diese Weise lassen sich mögliche Probleme mit Daten ausschließen. Sie können entscheiden, ob Sie die Daten zur Datenbank hinzufügen, die Daten einfach aus dieser Liste löschen oder das betreffende Element bei all zukünftigen Scans ignorieren wollen.
- **Software:** Öffnet das Dialogfeld **Softwarescaneinstellungen**. In diesem Dialogfeld konfigurieren Sie, wann der Softwarescan ausgeführt wird und wie lange das Inventarprotokoll gespeichert werden soll.
- **Attribute:** Öffnet das Dialogfeld **Attribute zum Speichern auswählen**, in dem Sie die Anzahl der in der Datenbank zu speichernden Inventarscanattribute begrenzen können. Hierdurch lässt sich die Größe der Datenbank reduzieren und die Einfügezeit für Scans verkürzen.
- **Duplikate verwalten: Geräte**: Öffnet das Dialogfeld **Doppelte Geräte**, in dem Sie festlegen können, wie mit doppelt vorhandenen Geräten zu verfahren ist.
- **Duplikate verwalten: Gerätekennungen:** Öffnet das Dialogfeld **Doppelte Gerätekennung**, in dem Sie Attribute auswählen können, mit denen Geräte eindeutig gekennzeichnet werden. Sie können mit dieser Option verhindern, dass doppelte Gerätekennungen in die Coredatenbank gescannt werden (siehe "Auflösen doppelter Gerätedatensätze in der Datenbank" auf Seite 88).
- **Status des Inventardiensts:** Zeigt an, ob der Dienst auf dem Coreserver gestartet oder angehalten wurde.
    - **Start:** Startet den Dienst auf dem Coreserver.
    - **Stopp:** Stoppt den Dienst auf dem Coreserver.
    - **Neustart:** Startet den Dienst auf dem Coreserver neu.

Informationen zum Dialogfeld "Unbekannte Inventarelemente"

Über das Dialogfeld **Unbekannte Inventarelemente** (**Konfigurieren > Dienste >** Registerkarte **Inventar >** Schaltfläche **Unbekannte Inventarelemente**) können Sie steuern, welche neuen Elemente zur Inventardatenbank hinzugefügt werden. Wenn der Inventarscan ausgeführt wird, kann er Objekte finden, die nicht in der Datenbank identifiziert sind. Da bei einem verwalteten Gerät beschädigte Daten oder andere Probleme vorliegen können, möchten Sie möglicherweise nicht, dass die neuen Daten zur Datenbank hinzugefügt werden. In diesem Dialogfeld werden alle Elemente aufgeführt, die gefunden wurden, und Sie haben die Möglichkeit, diese neuen Elemente zur Datenbank hinzuzufügen, zu löschen oder dafür zu sorgen, dass diese niemals zur Datenbank hinzugefügt werden.

- **Unbekannte Inventarelemente blockieren:** Wenn diese Kontrollkästchen aktiviert ist, werden alle unbekannten Element hier aufgeführt, bis Sie eine Entscheidung getroffen haben, wie damit zu verfahren ist.
- **Blockierte Elemente:** Listet all Inventarobjekte, die derzeit nicht in der Datenbank vorhanden sind. Klicken Sie zur Auswahl auf ein oder mehrere Elemente und wenden Sie eine Aktion an.
- **Zulassen:** Wählen Sie Elemente aus und klicken Sie auf **Zulassen**, um die Daten zur Datenbank hinzuzufügen. Die Elemente werden zur Datenbank hinzugefügt und können in zukünftigen Inventarscans verarbeitet werden.
- **Löschen:** Wählen Sie Elemente aus und klicken Sie auf **Löschen**, um sie nur aus dieser Liste zu löschen. Falls das Element erneut gefunden wird, erscheint es wieder in der Liste. Typischerweise würden Sie Elemente löschen, die das Ergebnis von Datenbeschädigungen sind, und diese Element würden dann auch niemals wieder in einem Scan gefunden.
- **Ignorieren:** Wählen Sie Elemente aus und klicken Sie auf **Ignorieren**, um zu dauerhaft zu unterbinden, dass diese zur Datenbank hinzugefügt werden. Die Liste "Ignorieren" sollte so kurz wie möglich gehalten werden, damit die Leistung des Systems nicht beeinträchtigt wird. Beachten Sie, dass alle Elemente in diese Liste permanent ignoriert werden. Die einzige Möglichkeit, sie aus dieser Liste zu entfernen, besteht darin, sie manuell aus der Tabelle META_IGNORE in der Inventardatenbank zu löschen und den Inventardienst neu zu starten.
- **OK/Abbrechen:** In diesem Dialogfeld gelten die Schaltflächen **OK** und **Abbrechen** nur für das Kontrollkästchen **Unbekannte Inventarelemente blockieren**, aber nicht für irgendwelche Aktionen im Zusammenhang mit blockierten Elementen.

Informationen zum Dialogfeld "Softwarescaneinstellungen"

Dieses Dialogfeld (**Konfigurieren > Dienste >** Registerkarte **Inventar** > Schaltfläche **Software**) verwenden Sie, um die Häufigkeit von Softwarescans zu konfigurieren. Die Hardware eines Geräts wird jedes Mal gescannt, wenn der Inventarscanner auf dem Gerät ausgeführt wird; die Software eines Geräts wird jedoch nur in den von Ihnen hier angegebenen Abständen gescannt.

- **Bei jeder Anmeldung:** Prüft bei jeder Anmeldung des Benutzers die gesamte Software, die auf dem Gerät installiert ist.
- **Einmal alle (Tage):** Prüft die auf dem Gerät installierte Software nur in dem angegebenen Tagesintervall (automatischer Scan).
- **Verlauf speichern (Tage):** Gibt an, wie lange der Inventarverlauf des Geräts gespeichert bleibt. Heben Sie die Markierung dieses Kontrollkästchens auf, wenn der Inventarverlauf nicht gespeichert werden soll.

Konfigurieren, welche Inventarscanattribute in der Datenbank gespeichert werden

Der Inventarscanner sucht nach Hunderten von Inventarelementen. Wenn Sie diese Scaninformationen nicht alle in Ihrer Datenbank benötigen, können Sie die Scaneinfügezeit beschleunigen und die Größe Ihrer Datenbank reduzieren, indem Sie die Anzahl der Scanattribute, die in der Datenbank gespeichert werden, limitieren. Wenn Sie dies tun, senden die verwalteten Geräte zwar weiterhin vollständige Inventarscans, jedoch speichert der Inventardienst des Coreservers nur die von Ihnen angegebenen Attribute in der Datenbank.

Standardmäßig fügt der Inventardienst alle Scanattribute in die Datenbank ein. Änderungen der Attributfilterung wirken sich nicht auf die bereits in Datenbank vorhandenen Daten aus. Um einzuschränken, welche Daten gespeichert werden, führen Sie die nachstehenden Schritte aus.

So richten Sie einen Inventarscan-Datenfilter ein

1. Klicken Sie auf **Konfigurieren > Dienste > Inventar**-Registerkarte **> Attribute**-Schaltfläche.
2. Attribute in der Spalte **Ausgewählte Attribute** auf der rechten Seite werden in die Datenbank eingefügt. Verschieben Sie die Attribute, die Sie nicht in der Datenbank speichern möchten, in die Spalte **Verfügbare Attribute** auf der linken Seite. Klicken Sie abschließend auf **OK**.
3. Starten Sie den Inventardienst neu, indem Sie auf der Registerkarte "Inventar" auf **Neu starten** klicken.
4. Klicken Sie auf **OK**.

Auflösen doppelter Gerätedatensätze in der Datenbank

In einigen Umgebungen ist die Betriebssystem-Abbilderstellung ein gängiges Verfahren zum Einrichten von Geräten. Damit geht eine erhöhte Wahrscheinlichkeit für doppelte Gerätekennungen auf den Geräten einher. Sie können dieses Problem vermeiden, indem Sie andere Geräteattribute spezifizieren, die in Kombination mit der Gerätekennung in der Lage sind, Ihre Geräte eindeutig zu kennzeichnen. Zu diesen anderen Attributen gehören beispielsweise Gerätename, Domänenname, BIOS, Bus, Coprozessor usw.

Mit der Funktion "Doppelte Kennung" können Sie Geräteattribute auswählen, die zur eindeutigen Kennzeichnung eines Geräts verwendet werden können. Sie geben an, um welche Attribute es sich handelt und wie viele von diesen Attributen identisch sein müssen, damit das Gerät als das Duplikat eines anderen Geräts ausgewiesen wird. Wenn der Inventarscanner ein identisches Gerät erkennt, schreibt er ein Ereignis in das Ereignisprotokoll der Anwendung, um auf die Gerätekennung des identischen Geräts zu verweisen.

Neben doppelten Gerätekennungen können sich auch doppelte Gerätenamen oder MAC-Adressen in der Datenbank ansammeln. Wenn wiederholt Probleme mit doppelten Gerätekennungen auftreten (und wenn Sie verhindern möchten, dass in der Zukunft doppelte Gerätedatensätze in Ihre Datenbank gescannt werden), können Sie angeben, dass doppelte Gerätenamen, die derzeit in der Datenbank enthalten sind, entfernt werden sollen. Diese zusätzliche Möglichkeit zur Handhabung doppelter Gerätekennungen ist Teil des nachstehend beschriebenen Verfahrens.

So konfigurieren Sie die Handhabung doppelter Geräte

1. Klicken Sie auf **Konfigurieren > Dienste > Inventar > Gerätekennungen**.
2. Wählen Sie aus der **Attributliste** die Attribute aus, die Sie verwenden möchten, um ein Gerät eindeutig zu kennzeichnen, und klicken Sie dann auf die Schaltfläche **>>**, um das Attribut zur Liste **Identitätsattribute** hinzuzufügen. Sie können beliebig viele Attribute hinzufügen.
3. Wählen Sie die Anzahl der Identitätsattribute (und Hardwareattribute) aus, für die ein Gerät fehlende Übereinstimmung melden muss, bevor es als Duplikat eines anderen Geräts ausgewiesen wird.
4. Wenn Sie möchten, dass doppelte Gerätekennungen vom Inventarscanner zurückgewiesen werden, aktivieren Sie die Option **Doppelte Kennungen ablehnen**.
5. Klicken Sie auf **OK**, um Ihre Einstellungen zu speichern und zum Dialogfeld **Inventar konfigurieren** zurückzukehren.
6. (Optional) Wenn Sie doppelt vorhandene Geräte auch nach dem Namen/der Adresse auflösen möchten, klicken Sie auf **Geräte**, um das Dialogfeld **Doppelte Geräte** zu öffnen. In diesem Dialogfeld können Sie die Bedingungen festlegen, unter denen doppelt vorhandene Geräte entfernt werden, beispielsweise wenn Gerätenamen, MAC-Adressen oder beide identisch sind.

Informationen zum Dialogfeld "Doppelte Gerätekennung"

Dieses Dialogfeld (**Konfigurieren > Dienste >** Registerkarte **Inventar >** Schaltfläche **> Gerätekennungen**) verwenden Sie, um die Handhabung doppelter Gerätekennungen festzulegen.

- **Attributliste:** Führt alle Attribute auf, die Sie auswählen können, um ein Gerät eindeutig zu kennzeichnen.
- **Identitätsattribute:** Zeigt die Attribute an, die Sie ausgewählt haben, um ein Gerät eindeutig zu kennzeichnen.
- **Doppelte Gerätekennung anmelden, wenn:** Bezeichnet die Anzahl der Attribute, für die ein Gerät Übereinstimmungen melden muss, damit es als Duplikat eines anderen Geräts ausgewiesen wird.
- **Doppelte Kennungen ablehnen:** Veranlasst den Inventarscanner, die Gerätekennung des doppelten Geräts aufzuzeichnen und alle nachfolgenden Versuche, diese Gerätekennung zu scannen, abzulehnen. Der Inventarscanner generiert daraufhin eine neue Gerätekennung.

Informationen zum Dialogfeld "Doppelte Geräte"

Dieses Dialogfeld (**Konfigurieren > Dienste > Inventar**-Registerkarte **> Geräte**-Schaltfläche klicken) verwenden Sie, um die Namens- und/oder Adressbedingungen anzugeben, unter denen doppelt vorhandene Geräte aus der Datenbank entfernt werden. Wenn Sie eine der Optionen zum Entfernen von Duplikaten aktiviert haben, sind Duplikate in der Datenbank zwar zulässig, jedoch werden sie bei der nächsten Datenbankwartung entfernt.

- **Doppelte Kennungen entfernen, wenn:**
  - **Gerätenamen übereinstimmen:** Entfernt den älteren Datensatz, wenn zwei oder mehr Gerätenamen in der Datenbank identisch sind.
  - **MAC-Adressen übereinstimmen:** Entfernt den älteren Datensatz, wenn zwei oder mehr MAC-Adressen in der Datenbank identisch sind.
  - **Gerätenamen und MAC-Adressen übereinstimmen:** Entfernt den älteren Datensatz nur, wenn mindestens zwei Gerätenamen und MAC-Adressen (für denselben Datensatz) identisch sind.
- **Ursprüngliche Gerätekennungen wiederherstellen:** Stellt die ursprüngliche Gerätekennung aus dem alten Datensatz eines gescannten Geräts wieder her, *wenn* zwei Datensätze für dieses Gerät in der Datenbank vorhanden sind und mindestens eine der oben angegebenen Optionen zum Entfernen ausgewählt und ihre Kriterien erfüllt sind. Die ursprüngliche Gerätekennung wird beim nächsten Inventarwartungsvorgang wiederhergestellt. Diese Option hat keine Auswirkungen, es sei denn, eine der o.g. Optionen zum Entfernen ist ausgewählt.

Konfigurieren des Scheduler-Dienstes

Auf der Registerkarte **Scheduler** konfigurieren Sie den Scheduler-Dienst (**Extras > Verteilung > Geplante Tasks**) für den Coreserver und die Datenbank, die Sie mithilfe der Registerkarte **Allgemein** ausgewählt haben.

Sie müssen über die entsprechenden Rechte verfügen, um diese Tasks auszuführen. Dies schließt das vollständige Administratorprivileg für die Windows-Geräte im Netzwerk ein, mit dem Sie diese Geräte berechtigen, Paketverteilungen vom Coreserver zu empfangen. Sie können mehrere auf den Geräten zu verwendende Sätze mit Anmeldeinformationen angeben, indem Sie auf **Anmeldung ändern** klicken.

Eine zusätzliche Einstellung, die Sie manuell konfigurieren können, ist die Aktualisierungsrate des Fensters **Geplante Tasks**. Standardmäßig überprüft das Fenster **Geplante Tasks** die Coredatenbank alle zwei Minuten, um zu bestimmen, ob eines der sichtbaren Elemente aktualisiert wurde. Wenn Sie die Aktualisierungsrate ändern möchten, navigieren Sie in der Registrierung zu folgendem Schlüssel:

- HKEY_CURRENT_USER\Software\LANDesk\ManagementSuite\WinConsole

Setzen Sie "TaskRefreshIntervalSeconds" auf die Anzahl von Sekunden zwischen Aktualisierungen für einen aktiven Task. Setzen Sie "TaskAutoRefreshIntervalSeconds" auf das Aktualisierungsintervall für das gesamte Fenster **Geplanter Task**.

Informationen zur Registerkarte "Scheduler"

Mithilfe dieser Registerkarte können Sie den Namen des Coreservers und der Datenbank anzeigen, die Sie zuvor ausgewählt haben, und die folgenden Optionen für einen geplanten Task festlegen:

- **Benutzername:** Der Benutzername, unter dem die geplanten Tasks ausgeführt werden. Er kann durch Klicken auf die Schaltfläche **Anmeldung ändern** geändert werden.
- **Zeit zwischen Wiederholungen (Sek.):** Wenn ein geplanter Task mit mehreren Wiederholungen konfiguriert wurde, wird mit dieser Einstellung festgelegt, wie viele Sekunden der Scheduler wartet, bevor er den Task wiederholt.
- **Zeit für Reaktivierungsversuche (Sek.):** Wenn ein geplanter Task mit Wake On LAN konfiguriert wurde, wird mit dieser Einstellung festgelegt, wie viele Sekunden der Dienst "Geplante Tasks" wartet, bevor er ein Gerät reaktiviert.
- **Intervall zwischen Abfrageevaluierungen:** Eine Zahl, die die Zeitspanne zwischen Abfrageauswertungen angibt, und eine Maßeinheit für die Zahl (Minuten, Stunden, Tage oder Wochen).
- **Wake-on-LAN-Einstellungen:** Der IP-Anschluss, der vom Wake-On-LAN-Paket verwendet wird, das von den geplanten Tasks zum Reaktivieren von Geräten festgelegt wurde.
- **Status des Scheduler-Diensts:** Zeigt an, ob der Scheduler-Dienst auf dem Coreserver gestartet oder angehalten wurde.
    - **Start:** Startet den Dienst auf dem Coreserver.
    - **Stopp:** Stoppt den Dienst auf dem Coreserver.
    - **Neustart:** Startet den Dienst auf dem Coreserver neu.
- **Erweitert:** Zeigt das Dialogfeld **Erweiterte Schedulereinstellungen** an. In diesem Dialogfeld können Sie andere, auf den Scheduler bezogene Einstellungen ändern. Beim Klicken auf die einzelnen Elemente werden Hilfetexte am unteren Rand des Dialogfelds eingeblendet, die die jeweilige Option beschreiben. Die Standardwerte sind für die meisten Installationen ausreichend. Um eine Einstellung zu ändern, klicken Sie auf die Einstellung, klicken Sie auf **Bearbeiten**, geben Sie einen neuen Wert ein und klicken Sie dann auf **OK**. Starten Sie nach Abschluss des Vorgangs den Scheduler neu.

Informationen zum Dialogfeld "Anmeldung ändern"

Das Dialogfeld **Anmeldung ändern** verwenden Sie, um die Standardanmeldung für den Scheduler zu ändern (**Konfigurieren > Dienste >** Registerkarte **Scheduler**). Sie können zudem auch alternative Anmeldeinformationen konfigurieren, die vom Scheduler-Dienst eingegeben werden sollten, wenn dieser einen Task auf nicht verwalteten Geräten ausführen muss.

Um LANDesk Agenten auf nicht verwalteten Geräten zu installieren, muss der Scheduler-Dienst in der Lage sein, mit einem administrativen Konto Verbindungen zu Geräten herzustellen. LocalSystem ist das vom Scheduler-Dienst verwendete Standardkonto. Die LocalSystem-Anmeldeinformationen funktionieren im Allgemeinen für Geräte, die sich nicht in der Domäne befinden. Bei Geräten, die sich in einer Domäne befinden, müssen Sie ein Domänenadministrator-Konto angeben.

Wenn Sie die Anmeldeinformationen für die Anmeldung des Scheduler-Dienstes ändern möchten, können Sie ein anderes Domänenebene-Verwaltungskonto zur Verwendung auf Geräten angeben. Wenn Sie Geräte über mehrere Domänen hinweg verwalten, können Sie zusätzliche Anmeldeinformationen hinzufügen, die der Scheduler-Dienst verwenden kann. Wenn Sie anstatt des LocalSystem-Kontos ein anderes Konto für den Scheduler-Dienst verwenden oder alternative Anmeldeinformationen anbieten möchten, müssen Sie eine primäre Scheduler-Dienst-Anmeldung angeben, die über Coreserver-Administratorrechte verfügt. Alternative Anmeldeinformationen benötigen keine Coreserver-Administratorrechte, müssen jedoch Administratorrechte auf Geräten besitzen.

Der Scheduler-Dienst versucht zunächst, sich mit den Standard-Anmeldeinformationen anzumelden. Wenn dies nicht gelingt, wiederholt er den Vorgang so lange mit allen Anmeldeinformationen, den Sie in der Liste **Alternative Anmeldeinformationen** angegeben haben, bis keine Anmeldeinformationen mehr vorhanden sind, mit denen er versuchen könnte, sich anzumelden. Von Ihnen angegebene Anmeldeinformationen werden verschlüsselt und in der Registrierung des Coreservers gespeichert.

HINWEIS: Rollup-Coreserver verwenden die Anmeldeinformationen des Scheduler-Diensts, um sich für die Synchronisierung zu authentifizieren. Auf Rollup-Cores müssen dies die Scheduler-Dienst-Anmeldeinformationen eines Mitglied einer Gruppe mit der Berechtigung eines Konsolenadministrators auf dem Quell-Coreserver sein. Wenn die Anmeldeinformationen nicht diesen Berechtigungen entsprechen, werden Sie im Synchronisierungsprotokoll des Quell-Coreservers Task-Handler-Fehler finden.

Sie können die folgenden Optionen für die Standard-Scheduler-Anmeldeinformationen festlegen:

- **Benutzername:** Geben Sie den Standarddomänennamen\Standardbenutzernamen oder den Benutzernamen ein, den der Scheduler verwenden soll.
- **Kennwort:** Geben Sie das Kennwort für den von Ihnen angegebenen Benutzernamen ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Sie können die folgenden Optionen für zusätzliche Scheduler-Anmeldeinformationen festlegen:

- **Hinzufügen:** Klicken Sie, um den neuen Benutzernamen und das neue Kennwort zur Liste **Alternative Anmeldeinformationen** hinzuzufügen.
- **Entfernen:** Klicken Sie, um die ausgewählten Anmeldeinformationen aus der Liste zu entfernen.
- **Ändern:** Klicken Sie, um die ausgewählten Anmeldeinformationen zu ändern.

Geben Sie beim Hinzufügen alternativer Anmeldeinformationen Folgendes an:

- **Benutzername:** Geben Sie den Benutzernamen ein, den der Scheduler verwenden soll.
- **Domäne:** Geben Sie die Domäne für den von Ihnen angegebenen Benutzernamen ein.
- **Kennwort:** Geben Sie das Kennwort für die von Ihnen festgelegten Anmeldeinformationen ein.
- **Kennwort bestätigen:** Geben Sie das Kennwort erneut ein, um es zu bestätigen.

Konfigurieren des Dienstes für benutzerdefinierte Tasks

Konfigurieren Sie mithilfe der Registerkarte **Benutzerdefinierte Tasks** den Dienst für benutzerdefinierte Tasks für den Coreserver und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben. Zu den benutzerdefinierten Tasks gehören beispielsweise Inventarscans, Gerätebereitstellungen oder Softwareverteilungen.

Tasks können über eines der beiden Protokolle für die Remoteausführung ausgeführt werden, d. h. entweder das TCP-Protokoll oder das standardmäßige LANDesk Agentenprotokoll. Wenn Sie die TCP-Remoteausführung als Remoteausführungsprotokoll deaktivieren, verwendet die Option "Benutzerdefinierte Tasks" standardmäßig das Protokoll des LANDesk Standardagenten, unabhängig davon, ob es als deaktiviert gekennzeichnet ist oder nicht. Wenn sowohl die TCP-Remoteausführung als auch der LANDesk Standardagent aktiviert sind, versucht der Dienst "Benutzerdefinierte Tasks" zuerst, die TCP-Remoteausführung zu verwenden. Wenn diese nicht vorhanden ist, wird die LANDesk Standardagent-Remoteausführung verwendet.

Auf der Registerkarte **Benutzerdefinierte Tasks** können Sie Optionen für die Erkennung von Geräten auswählen. Damit die benutzerdefinierte Taskverarbeitung einen Task bearbeiten kann, muss sie die aktuelle IP-Adresse des Geräts ausfindig machen. Mit dieser Registerkarte können Sie festlegen, wie der Dienst mit den Geräten Kontakt aufnimmt.

Informationen zum Dialogfeld "LANDesk Softwaredienste konfigurieren: Registerkarte 'Benutzerdefinierte Tasks'"

Definieren Sie mithilfe dieser Registerkarte die folgenden Optionen für benutzerdefinierte Tasks:

Remoteausführungsoptionen:

- **TCP-Ausführung deaktivieren:** Deaktiviert TCP als Remoteausführungsprotokoll und verwendet standardmäßig das LANDesk Agentenprotokoll.
- **CBA-Ausführung/Dateiübertragung deaktivieren:** Deaktiviert den LANDesk Standardagenten als Remoteausführungsprotokoll. Wenn der LANDesk Standardagent deaktiviert ist und das TCP-Remoteausführungsprotokoll nicht auf dem Gerät gefunden wird, misslingt die Remoteausführung.
- **Timeout für Remoteausführung aktivieren:** Aktiviert ein Zeitlimit für die Remoteausführung und legt fest, nach wie vielen Sekunden ein Timeout erfolgt. Zeitlimits für die Remoteausführung werden ausgelöst, wenn das Gerät Heartbeat-Signale sendet, der Task auf dem Gerät jedoch hängen geblieben ist oder sich in einer Schleife befindet. Diese Einstellung gilt für beide Protokolle (TCP oder Standard LANDesk Agent). Dieser Wert kann zwischen 300 Sekunden (5 Minuten) und 86400 Sekunden (1 Tag) liegen.
- **Clienttimeout aktivieren:** Aktiviert ein Geräte-Timeout und legt fest, nach wie vielen Sekunden das Timeout stattfindet. Standardmäßig sendet die TCP-Remoteausführung ein Heartbeat-Signal vom Gerät an den Server in Intervallen von 45 Sekunden, bis die Remoteausführung abgeschlossen ist oder ein Timeout erfolgt. Gerätetimeouts werden ausgelöst, wenn das Gerät kein Heartbeat-Signal an den Server sendet.
- **Remoteausführungsport:** Gibt den Port an, über den die TCP-Remoteausführung erfolgt. Standard ist 12174. Wenn dieser Port geändert wird, muss er auch in der Gerätekonfiguration geändert werden.

Verteilungsoptionen

- **Verteilen an <nn> Computer gleichzeitig:** Gibt die maximale Anzahl von Geräten an, an die benutzerdefinierte Aufträge gleichzeitig verteilt werden.

Erkennungsoptionen

- **UDP:** Wenn Sie UDP auswählen, wird ein LANDesk Agent-Ping über UDP verwendet. Die meisten LANDesk Gerätekomponenten sind auf den Standard LANDesk Agenten angewiesen. Aus diesem Grund sollte auf Ihren verwalteten Geräten der Standard LANDesk Agent installiert sein. Dies ist die schnellste Erkennungsmethode und gleichzeitig der Standard. Mit UDP können Sie auch die Anzahl der **Wiederholungen** und das **Timeout** für den UDP-Ping auswählen.
- **TCP:** Wählen Sie TCP aus, um eine HTTP-Verbindung mit dem Gerät auf Port 9595 zu verwenden. Diese Erkennungsmethode hat den Vorteil, dass sie über eine Firewall hinweg einsatzfähig ist, wenn Sie Port 9595 öffnen; die Methode unterliegt jedoch HTTP-Verbindungs-Timeouts, wenn keine Geräte vorhanden sind. Diese Timeouts können 20 Sekunden oder länger beanspruchen. Wenn eine große Zahl von Zielgeräten nicht auf die TCP-Verbindung reagiert, dauert es einige Zeit, bis Ihr Task gestartet werden kann.
- **Beide:** Wählen Sie "Beide" aus, wenn der Dienst die Erkennung erst mit UDP, dann mit TCP und zuletzt mit DNS/WINS (sofern ausgewählt) versuchen soll.
- **Subnetz-Broadcast deaktivieren:** Wenn Sie diese Option auswählen, wird die Erkennung über ein Subnetz-Broadcast deaktiviert. Wenn ausgewählt, veranlasst diese Option die Weiterleitung eines Subnetz-gesteuerten Broadcast über UDP unter Verwendung von PDS.
- **DNS/WINS-Lookup deaktivieren:** Wenn diese Option ausgewählt ist, deaktiviert sie einen Name Service Lookup für jedes Gerät, wenn die ausgewählte TCP/UDP-Erkennungsmethode scheitert.

Konfigurieren des Multicast-Dienstes

Auf der Registerkarte **Multicast** konfigurieren Sie die Erkennungsoptionen für Multicast-Domänenrepräsentanten für den Coreserver und die Datenbank, die Sie mithilfe der Registerkarte "Allgemein" ausgewählt haben.

Informationen zur Registerkarte "Multicast"

Definieren Sie mithilfe dieser Registerkarte die folgenden Multicast-Optionen:

- **Multicast-Domänenrepräsentanten verwenden:** Verwendet die Liste mit den Multicast-Domänenrepräsentanten, die in der Gruppe **Konfiguration > Multicast-Domänenrepräsentanten** der Netzwerkansicht enthalten ist.
- **Cachedatei verwenden:** Fragt jede Multicast-Domäne ab, um herauszufinden, wer die Datei bereits besitzt; in diesem Fall wird die Datei nicht auf einen Repräsentanten heruntergeladen.
- **Cachedatei vor bevorzugtem Domänenrepräsentanten verwenden:** Ändert die Reihenfolge der Erkennung so, dass **Cachedatei verwenden** die erste Option ist, die zur Anwendung kommt.
- **Broadcast verwenden:** Sendet einen Subnetz-Broadcast, um alle Geräte in dem betreffenden Subnetz zu finden, die Multicast-Domänenrepräsentanten sein könnten.
- **Protokoll-Verwerfungszeitraum (Tage):** Gibt an, für wie viele Tage Einträge im Protokoll aufbewahrt werden, bevor sie gelöscht werden.

Konfigurieren des Dienstes für die Betriebssystembereitstellung

Auf der Registerkarte **Betriebssystembereitstellung** können Sie PXE-Repräsentanten als PXE-Warteschlangen deklarieren und grundlegende PXE-Boot-Optionen für den Coreserver und die Datenbank konfigurieren, die Sie auf der Registerkarte "Allgemein" ausgewählt haben.

PXE-Warteschlangen sind eine Methode für die Bereitstellung von Betriebssystemabbildern auf PXE-kompatiblen Geräten. Sie erklären vorhandene PXE-Repräsentanten (in der Gruppe **Konfiguration** der Netzwerkansicht) als PXE-Warteschlangen. Weitere Informationen finden Sie unter "PXE-basierte Bereitstellung – Übersicht" auf Seite 385.

Wählen Sie die PXE-Repräsentanten aus und verschieben Sie sie aus der Liste **Verfügbare Proxys** in die Liste **Warteschlangen-Proxys**.

Informationen zur Registerkarte "Betriebssystembereitstellung"

Verwenden Sie diese Registerkarte, um PXE-Warteschlangen-Proxys (Repräsentanten) zuzuweisen und die PXE-Boot-Optionen zu definieren.

- **Verfügbare Proxys:** Führt alle im Netzwerk verfügbaren PXE-Proxys anhand ihres Gerätenamens auf. Diese Liste wird generiert, wenn der Inventarscanner PXE-Software (PXE- und MTFTP-Protokolle) erkennt, die auf dem Gerät ausgeführt wird.
- **Warteschlangen-Proxys:** Führt die PXE-Proxys auf, die von der Liste **Verfügbare Proxys** verschoben wurden und den Proxy als PXE-Haltewarteschlange deklarieren. PXE-taugliche Geräte im selben Subnetz wie der PXE-Warteschlangen-Proxy werden automatisch der Gruppe mit den **PXE-Warteschlangen** in der Netzwerkansicht der Konsole hinzugefügt, wenn für sie ein PXE-Boot durchgeführt wird. Anschließend kann für die Geräte ein Abbildbereitstellungsauftrag geplant werden.
- **Zurücksetzen:** Zwingt alle PXE-tauglichen Geräte, die sich im selben Subnetz wie der ausgewählte PXE-Repräsentant befinden, die Gruppe **PXE-Warteschlange** wieder in die Netzwerkansicht der Konsole einzufügen. Für diese Geräte kann dann ein Abbildverarbeitungsauftrag geplant werden. (Die Schaltfläche "Zurücksetzen" wird aktiviert, wenn Sie einen PXE-Proxy in der Liste "Warteschlangen-Proxys" auswählen.)

HINWEIS: Änderungen, die Sie hier an den PXE-Boot-Optionen vornehmen, wirken sich erst dann auf die PXE-Repräsentanten aus, wenn Sie das Skript "PXE Representative Deployment" auf diesem Repräsentanten ausführen.

- **Timeout:** Gibt an, wie lange die Start-Eingabeaufforderung bis zum Timeout angezeigt und wann der Standardstartvorgang wieder aufgenommen wird. Es können maximal 60 Sekunden eingegeben werden.
- **Meldung:** Legt den PXE-Boot-Prompt fest, der auf dem Gerät angezeigt wird. Sie können jede beliebige Meldung in das Textfeld eingeben, bis zu einer maximalen Länge von 75 Zeichen.

Validieren der Prebootumgebung für die Betriebssystembereitstellung

Klicken Sie auf die Schaltfläche **OSD-Validierung**, um das Dialogfeld **OSD-Abbilderstellungsumgebung** aufzurufen, in dem Sie Ihre Lizenz zur Verwendung einer DOS- oder Windows-Prebootumgebung für die Betriebssystembereitstellung validieren können.

Informationen zum Dialogfeld "OSD-Abbilderstellungsumgebung"

Das Dialogfeld **OSD-Abbilderstellungsumgebung** verwenden Sie, um Ihre Lizenz für die Verwendung einer DOS- oder Windows-Prebootumgebung zu validieren. Dies sind die Anforderungen für die Lizenzvalidierung:

- **Windows PE:** Wenn Sie auf die Schaltfläche "Lizenz" klicken, werden Informationen zur der in diesem Produkt enthaltenen Windows PE-Lizenz angezeigt. Sie müssen die Lizenzbedingungen akzeptieren, erst dann können Sie Windows PE in Verbindung mit der Betriebssystembereitstellung

oder der Versorgung verwenden.

- **DOS:** Die Lizenzverifizierung erfordert eine Windows NT 4 Server- und eine Windows 98-CD.

So validieren Sie eine DOS-PE-Umgebung

1. Klicken Sie auf der Registerkarte **Betriebssystembereitstellung** auf die Schaltfläche **OSD-Validierung**. (Wenn Sie das Extra zur Betriebssystembereitstellung verwenden, klicken Sie in der Symbolleiste auf die Schaltfläche **Lizenzen validieren**.)
2. Klicken Sie im Abschnitt **DOS-Abbilderstellungsumgebung** auf **Jetzt verifizieren**.
3. Legen Sie eine Windows NT4 Server-Installations-CD in ein Laufwerk ein. Klicken Sie auf **Durchsuchen** und wählen Sie den Ordner \CLIENTS\MSCLIENT\DISKS auf der CD aus.
4. Klicken Sie auf **OK**. Der Validierungsprozess greift auf die Dateien auf dieser CD zu. Nach Abschluss dieses Vorgangs werden Sie aufgefordert, die nächste CD einzulegen.
5. Wenn die Aufforderung erscheint, legen Sie eine Windows 98-Installations-CD in ein Laufwerk ein. Klicken Sie auf **Durchsuchen** und wählen Sie den Ordner \WIN98 auf der CD aus.
6. Klicken Sie auf **OK**. Der Validierungsprozess wird fortgesetzt. Wenn er abgeschlossen ist, klicken Sie auf **OK**.

So akzeptieren Sie die Lizenz für die Windows PE-Umgebung

1. Klicken Sie auf der Registerkarte **Betriebssystembereitstellung** auf die Schaltfläche **OSD-Validierung**. (Wenn Sie das Extra zur Betriebssystembereitstellung verwenden, klicken Sie in der Symbolleiste auf die Schaltfläche **Lizenzen validieren**.)
2. Klicken Sie im Abschnitt **Windows PE-Lizenzvereinbarung** auf **Lizenz**.
3. Klicken Sie auf den Link, um die Bedingungen der WAIK-Lizenz zu akzeptieren. Im Dialogfeld "OSD-Abbilderstellungsumgebung" erscheint die Meldung "Akzeptiert".

WICHTIG: Dieses Produkt installiert im Rahmen der Produktinstallation Komponenten aus dem Windows Automated Installation Kit (WAIK) für Windows 7, darunter auch eine Windows PE-Umgebung. Installieren Sie keinesfalls eine andere Version des WAIK auf Ihrem Coreserver, sonst kann es zu Konflikten zwischen den beiden WAIK-Versionen kommen. Wenn Sie eine andere Version des WAIK verwenden möchten, installieren Sie diese auf einem anderen Computer als Ihrem Coreserver.

So wählen Sie eine Standard-Prebootumgebung (PE) aus

1. Nachdem Sie die Prebootumgebungen, die Sie verwenden möchten, verifiziert haben, kehren Sie zum Dialogfeld "OSD-Abbilderstellungsumgebung" zurück.
2. Wählen Sie in der Liste **Standard-Prebootumgebung (PE)** entweder **DOS**, **Linux** oder **Windows** als Ihre Standard-Prebootumgebung aus.
3. Klicken Sie auf **OK**.

Konfigurieren des BMC-Kennworts

Die Registerkarte **BMC-Kennwort** verwenden Sie, um ein Kennwort für den IPMI Baseboard Management Controller (BMC) bei IPMI-fähigen Geräten zu erstellen.

- **Kennwort:** Geben Sie das Kennwort ein, das als BMC-Kennwort auf IPMI-Geräten verwendet werden soll.

- **Kennwort bestätigen:** Geben Sie das Kennwort in dieses Textfeld ein und klicken Sie dann auf **Übernehmen** oder auf **OK**, um das Kennwort festzulegen.

Das Kennwort darf maximal 15 Zeichen umfassen und keine anderen Zeichen als die Ziffern 0 bis 9 und die Groß- oder Kleinbuchstaben A bis Z enthalten.

Konfigurieren der Anmeldeinformationen für die Betriebssystem-Virtualisierung

Die Registerkarte **Betriebssystem-Virtualisierung** verwenden Sie, um die Standard-Anmeldeinformationen zur Verwaltung von VMware ESX-Servern einzugeben, die als virtuelle Hosts konfiguriert sind. Virtuelle Betriebssystemhosts, die erkannt wurden, werden in der Netzwerkansicht in einem separaten Ordner namens **Virtuelle Betriebssystemhosts** angezeigt.

- **Benutzername:** Geben Sie den Standardbenutzernamen ein.
- **Kennwort/Kennwort bestätigen:** Geben Sie das zu verwendende Kennwort und die Kennwortbestätigung ein und klicken Sie dann auf **Übernehmen** oder auf **OK**, um die Anmeldeinformationen festzulegen.

Coresynchronisierung

Coresynchronisierung

Mit der Coresynchronisierung können Sie Konfigurationen und Tasks manuell oder automatisch von einem Core auf einen anderen Core kopieren. Die Funktion kann dazu verwendet werden, mehrere Cores in synchronisiertem Zustand zu einem Mastercore zu halten.

Folgende Elemente können synchronisiert werden:

- Agentenkonfigurationen
- Alarme
- Spaltensätze
- Verteilungsmethoden
- Verteilungspakete
- Energieverwaltungseinstellungen
- Abfragen und Abfragespalteneinstellungen
- Skripte
- Agenteneinstellungen (**HINWEIS:** Vormals "Security- und Patch-Einstellungen)
- Tasks und Richtlinien

Es gibt drei Möglichkeiten für die Synchronisierung von Elementen:

- Bei Bedarf
- Automatisch
- Import/Export

Wenn Sie Tasks oder Softwareverteilungspaket-Konfigurationen exportieren bzw. synchronisieren, enthalten die exportierten bzw. synchronisierten Daten verknüpfte Abfragen und zugehörige Elemente. Beachten Sie, dass die exportierten/synchronisierten Daten nur Informationen aus der Management Suite Datenbank enthalten. Exportdateien zur Softwareverteilung enthalten beispielsweise nicht das eigentliche Verteilungspaket.

Diesbezüglich sollten Sie beim Einsatz von geplanten Tasks für den Export bzw. die Synchronisierung sicherstellen, dass alle Paketpfade für die Quell- und die Zielserver übereinstimmen. Sonst könnte es passieren, das ein Task bei seinem Import bzw. seiner Synchronisierung fehlschlägt, weil der Zielserver das Paket nicht finden konnte.

Beim Kopieren oder automatischen Synchronisieren eines Element geschieht Folgendes:

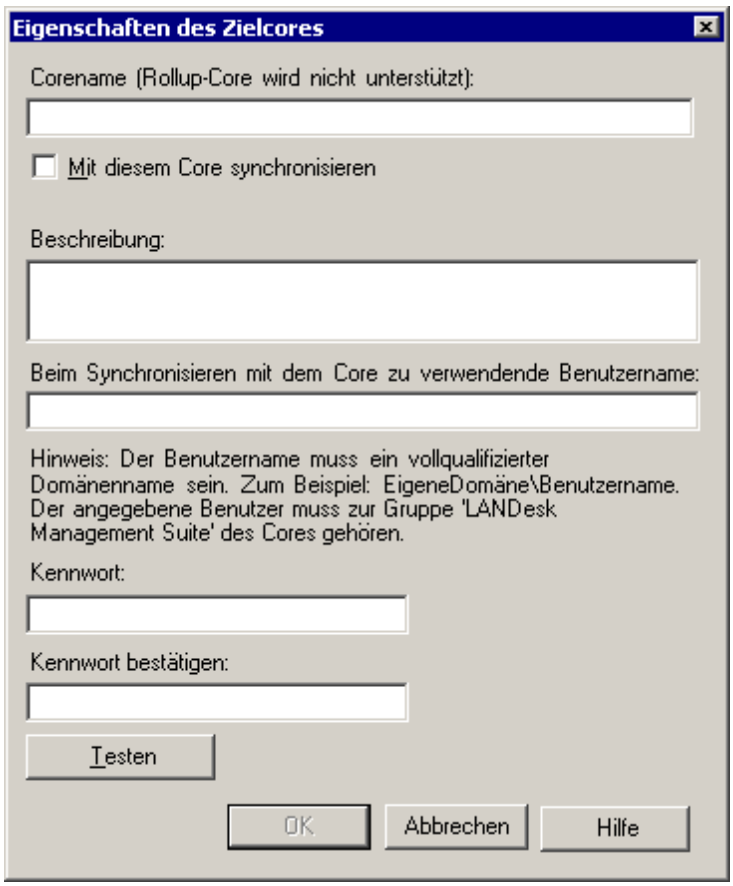
1. Der Quell-Coreserver erstellt eine .ldms-Exportdatei im XML-Format, die alle notwendigen Informationen zur Neuerstellung des Quellelements und aller anderen Elemente enthält, auf das sich das Quellelement bezieht.
2. Der Quell-Coreserver stellt über HTTPS eine Verbindung zum sicheren Webdienst des Ziel-Coreservers her und überträgt die .ldms-Datei.
3. Der sichere Webdienst des Ziel-Coreservers kopiert die empfangene .ldms-Datei in seinen Order C:\Programme\LANDesk\ManagementSuite\exportablequeue.

4. Der Coresynchronisierungsdienst kontrolliert diesen Order in regelmäßigen Abständen auf neue Dateien. Er findet die vom Quellcore exportierte Datei und importiert sie, wobei er die Datei aus dem Ordner entfernt.

HINWEIS: Die Tools zur Betriebssystembereitstellung und zur Softwarelizenzüberwachung bieten keine Unterstützung für die Coresynchronisierung.

Hinzufügen von Servern zur Coresynchronisierungsliste

Bevor Sie mit der Coresynchronisierung arbeiten können, müssen Sie die Liste der Server konfigurieren, mit denen eine Synchronisierung erfolgen soll. Cores kommunizieren über HTTPS und authentifizieren sich mit einem Benutzernamen und einem Kennwort, den bzw. das Sie für alle Cores bereitstellen.


Eigenschaften des Zielcores
Corename (Rollup-Core wird nicht unterstützt):
Mit diesem Core synchronisieren
Beschreibung:
Beim Synchronisieren mit dem Core zu verwendende Benutzername:
Hinweis: Der Benutzername muss ein vollqualifizierter Domänenname sein. Zum Beispiel: EigeneDomäne\Benutzername. Der angegebene Benutzer muss zur Gruppe 'LANDesk Management Suite' des Cores gehören.
Kennwort:
Kennwort bestätigen:
Testen
OK
Abbrechen
Hilfe

So fügen Sie einen Coreserver zur Synchronisierungsliste hinzu

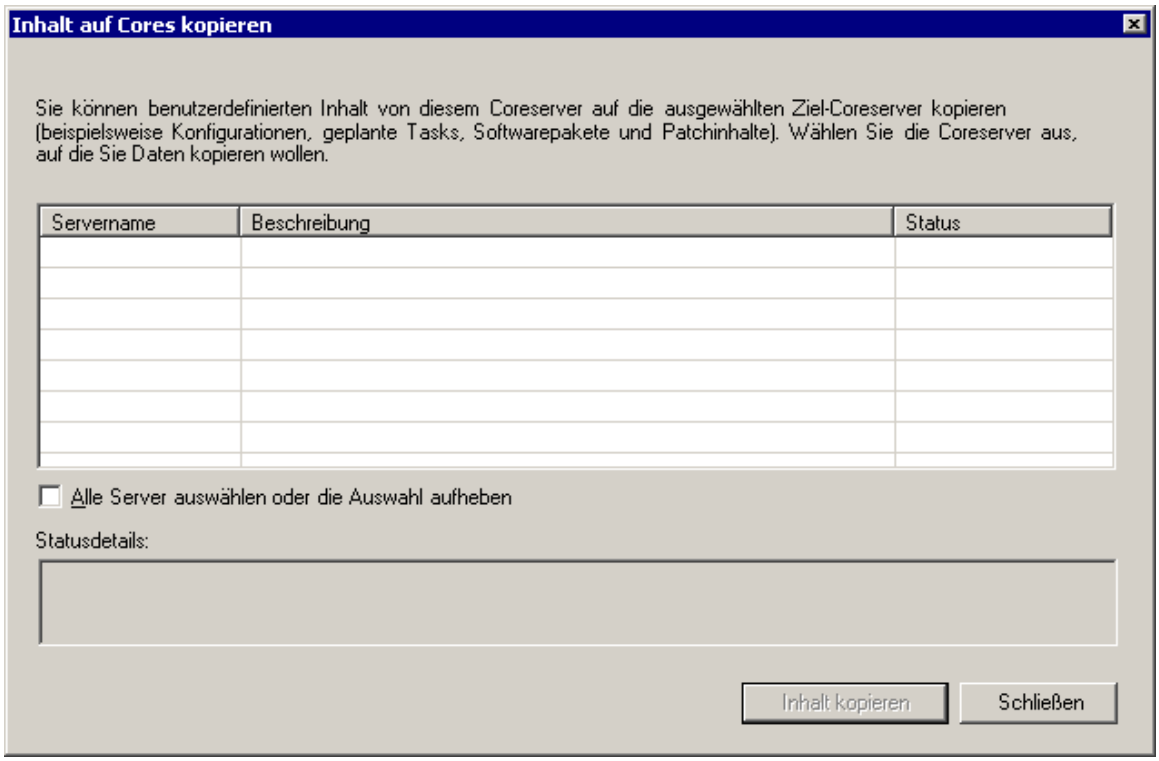
1. Klicken Sie auf **Extras > Administration > Coresynchronisierung**.
2. Klicken Sie mit der rechten Maustaste auf das Baumelement **Coreserver** und klicken Sie dann auf **Zielcore hinzufügen**.
3. Geben Sie den **Corenamen** ein.

4. Wählen Sie **Mit diesem Core synchronisieren** aus, um die Coresynchronisierung beim Verlassen des Dialogfelds zu aktivieren. Sie können diese Option auch später auswählen oder die Auswahl wieder aufheben, um die Synchronisierung mit diesem Core selektiv zu aktivieren bzw. zu deaktivieren.
5. Geben Sie eine **Beschreibung** ein.
6. Geben Sie den vollqualifizierten Domänennamen (FQDN) für das Benutzerkonto ein, das bei der Synchronisierung verwendet werden soll (Domäne\Benutzername). Dieses Konto muss über eine volle Konsolenberechtigung verfügen und Mitglied einer der lokalen LANDesk Benutzergruppen auf dem Zielcore sein.
7. Geben Sie das **Kennwort** und die Kennwortbestätigung für das von Ihnen angegebene Konto ein.
8. Klicken Sie auf **Testen**, um Ihre Konfiguration zu bestätigen.
9. Klicken Sie auf **OK**.

WICHTIG: Rollup-Coreserver verwenden die Anmeldeinformationen des Scheduler-Diensts, um sich für die Synchronisierung zu authentifizieren. Auf Rollup-Cores müssen dies die Scheduler-Dienst-Anmeldeinformationen eines Mitglied einer Gruppe mit der Berechtigung eines Konsolenadministrators auf dem Quell-Coreserver sein. Wenn die Anmeldeinformationen nicht diesen Berechtigungen entsprechen, werden Sie im Synchronisierungsprotokoll des Quell-Coreservers Task-Handler-Fehler finden. Information darüber, wie die Anmeldeinformationen des Scheduler-Diensts geändert werden können, finden Sie unter "Informationen zum Dialogfeld "Anmeldung ändern"" auf Seite 90.

Elemente bei Bedarf synchronisieren

Mit der Coresynchronisierung können ein Element bei Bedarf synchronisieren, indem Sie mit der rechten Maustaste darauf klicken und dann auf **Auf anderen Core bzw. andere Cores kopieren** klicken. Hierbei können Sie die Server auswählen, die die Kopie erhalten sollen. Wenn Sie auf **Inhalt kopieren** klicken, beginnt sofort der Kopiervorgang. Der Kopiervorgang findet nur einmal statt und das kopierte Element steht sofort auf den Remote-Cores zu Verfügung. Beachten Sie, dass Sie unter Umständen die Konsolenansicht des Remote-Cores durch Drücken der Taste F5 aktualisieren müssen, damit das Element angezeigt wird. Die Remotekopien haben denselben Namen und Speicherort wie die Quellkopie und können bearbeitet werden. Gruppen oder Untergruppen, die das Element enthalten, werden automatisch erstellt.


Inhalt auf Cores kopieren
Sie können benutzerdefinierten Inhalt von diesem Coreserver auf die ausgewählten Ziel-Coreserver kopieren (beispielsweise Konfigurationen, geplante Tasks, Softwarepakete und Patchinhalte). Wählen Sie die Coreserver aus, auf die Sie Daten kopieren wollen.
Servername
Beschreibung
Status
Alle Server auswählen oder die Auswahl aufheben
Statusdetails:
Inhalt kopieren
Schließen

Automatisches Synchronisieren von Elementen

Bevor Sie die automatische Synchronisierung verwenden, konfigurieren Sie, welche Komponenten von Management Suite synchronisiert werden sollen.

Konfigurieren der automatischen Synchronisierung

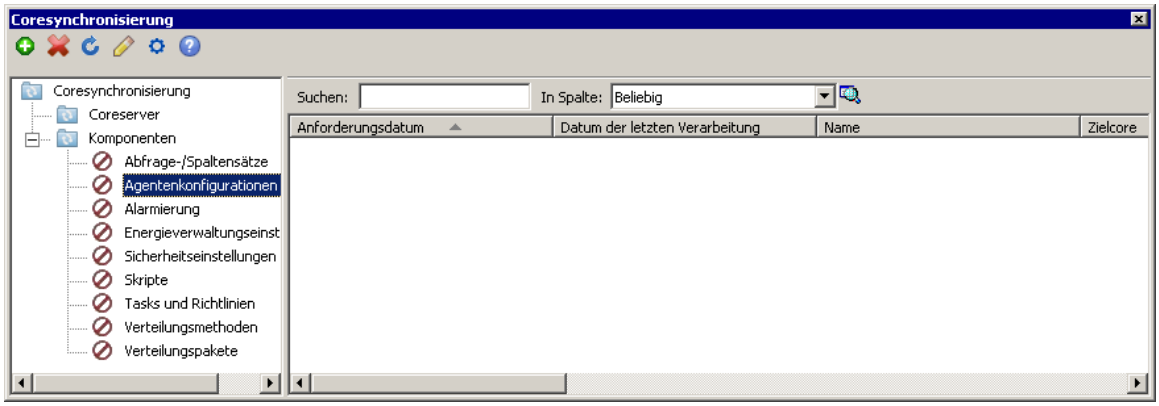
Sie können die automatische Synchronisierung für einzelne Elementen aktivieren. Wenn jedoch bei einer Komponente eines Elements die Synchronisierungsfunktion nicht aktiviert ist, wird dieses Element nicht synchronisiert. Wird die Synchronisierung auf einer Komponente deaktiviert, so ändert sich dadurch das Flag für die automatische Synchronisierung bei den mit dem Flag gekennzeichneten Elementen nicht. Das heißt, wenn Sie die Synchronisierung deaktivieren und später wieder aktivieren, wird die Synchronisierung von Elementen, für die Sie die automatische Synchronisierung ursprünglich aktiviert hatten, wieder aufgenommen.

So wählen Sie die Komponenten aus, die für die automatische Synchronisierung aktiviert werden sollen

1. Klicken Sie auf **Extras > Administration > Coresynchronisierung**.
2. Klicken Sie mit der rechten Maustaste auf das Baumelement **Komponenten** und klicken Sie dann auf **Automatische Synchronisierungskomponenten bearbeiten**.
3. Verschieben Sie die Komponenten, die synchronisiert werden sollen, in die Liste **Automatische Synchronisierung**.
4. Klicken Sie auf **OK**.

Sie können die automatische Synchronisierung auch aktivieren oder deaktivieren, indem Sie mit der rechten Maustaste auf eine Komponente klicken und dann **Automatische Synchronisierung** wählen.

Wenn Sie im Baum **Komponenten** eine Komponente auswählen, können Sie die Synchronisierungsaktivität für diese Komponente einsehen.



Aktivieren der automatischen Synchronisierung für ein Element

Sie können ein Element automatisch synchronisieren, indem Sie mit der rechten Maustaste in der Baumansicht einer Komponente klicken und **Automatische Synchronisierung** wählen. Wenn die Synchronisierungskomponente eines Elements nicht aktiviert ist, werden Sie aufgefordert, diese Komponente zu aktivieren. Die Synchronisierung für dieses Element findet beim nächsten Synchronisierungsintervall statt. Wenn Sie nochmals mit der rechten Maustaste auf dieses Element klicken, erscheint im Menü ein Häkchen neben **Automatische Synchronisierung**.

Wie auch bei der bei Bedarf ("On-Demand") durchgeführten Synchronisierung erscheinen die automatisch synchronisierten Elemente am selben Speicherort in der Konsole. Automatisch synchronisierte Elemente sind jedoch auf Zielcores schreibgeschützt und können daher weder bearbeitet noch gelöscht werden. Jedes Mal, wenn Sie ein automatisch synchronisiertes Element auf dem Quellcore ändern, wird dieses Element mit den Zielcores synchronisiert. Wenn Konsolenbenutzern die Möglichkeit gegeben werden soll, ein automatisch synchronisiertes Element zu löschen, schalten Sie einfach die automatische Synchronisierung aus. Das Element wird dadurch nicht von den Zielcores entfernt, aber diese Zielelemente können dann bearbeitet werden.

Synchronisieren von geplanten Tasks

Die Daten zu einem synchronisierten geplanten Task enthalten keine Daten zur Startzeit des Tasks. Wenn Sie einen geplanten Task synchronisieren, können Sie ihn auf dem Zielserver nur ausführen, wenn Sie mit der rechten Maustaste darauf klicken und **Jetzt starten** auswählen. Da synchronisierte Elemente schreibgeschützt sind, können Sie diese auf dem Zielcore nicht bearbeiten und eine neue Startzeit hinzufügen. Zur Umgehung des Problems können Sie die Funktion "Auf Core(s) kopieren" verwenden. Der Task enthält dann auf dem Zielcore zwar immer noch keine Startzeit, aber er kann auf diese Weise wenigstens dort bearbeitet werden.

Exportieren und Importieren von Coresynchronisierungselementen

Elemente die synchronisiert werden können, lassen sich ebenfalls exportieren und importieren. Beim Exportieren eines Elements wird eine .ldms-Datei im XML-Format erstellt, die alle notwendigen Daten zur Neuerstellung des Elements und aller anderen Elemente enthält, auf das sich dieses Element bezieht. Sie können diese Datei dann beispielsweise auf einen anderen Core verlegen und wieder importieren.

Beim Importieren werden Sie aufgefordert, eine der folgenden drei Maßnahmen zu ergreifen:

- **Aktualisieren:** Fügt übereinstimmende Elemente ein oder aktualisiert diese, wobei die in der .ldms-Datei festgelegte Gruppenhierarchie erhalten bleibt. Die Kennungen aus der Datei werden beibehalten. Hiermit werden sämtliche Änderungen am bestehenden Element überschrieben.
- **Elemente in die ausgewählte Gruppe oder den ausgewählten Eigentümer einfügen:** Fügt alle Elemente ein und weist jedem Element eine neue Kennung zu. Ein Hinzufügen zur Gruppe erfolgt nur bei übereinstimmendem Typ. Der Eigentümer jedes importierten Elements wird aktualisiert.
- **Elemente in die in der .ldms-Datei definierte(n) Gruppe(n) einfügen** Fügt die neuen Elemente ein, wobei die in der .ldms-Datei festgelegte Gruppenhierarchie erhalten bleibt. Jedem Element wird eine neue Kennung zugewiesen.

Nähere Informationen darüber, wie Konfliktmanagement funktioniert, finden Sie unter "Konfliktmanagement bei der Coresynchronisierung" auf Seite 103.

So exportieren Sie ein Element

1. Klicken Sie in der **Netzwerkansicht** oder der Baumansicht des Extras mit der rechten Maustaste auf das Element, das Sie exportieren möchten und klicken Sie dann auf **Exportieren**. Wenn ein Element exportiert werden kann, weist das Kontextmenü den Befehl **Exportieren** auf.
2. Geben Sie einen Dateinamen ein und navigieren Sie zum gewünschten Verzeichnispfad.
3. Klicken Sie auf **Speichern**.

So importieren Sie ein Element

1. Navigieren Sie in der **Netzwerkansicht** oder der Baumansicht des Extras zu dem Speicherort, an dem das importiere Element erscheinen soll.
2. Klicken Sie mit der rechten Maustaste und wählen Sie **Kopieren**.
3. Klicken Sie auf die gewünschte Importoption.
4. Klicken Sie auf **Importieren**.

Überwachen des Coresynchronisierungsstatus

Wenn Sie in der Strukturansicht des Extras "Coresynchronisierung" einen **Coreserver** oder eine **Komponente** auswählen, können Sie ein Protokoll zu den Synchronisierungen und den Echtzeit-Synchronisierungsstatus einsehen. Blättern Sie nach rechts, um die verfügbaren Statusspalten anzuzeigen. Wenn Sie den Stammknoten **Coreserver** auswählen, können Sie den Synchronisierungsstatus für Zielcores auf höchster Ebene anzeigen. Die zugehörigen Daten geben Aufschluss über die ausstehende Anzahl von Synchronisierungen. Ein hoher Wert oder keine Veränderung kann auf ein Problem bei der Synchronisierung auf dem betreffenden Core hindeuten.

Synchronisierte Elemente können einen der folgenden Status aufweisen:

- **Ausstehend:** Das Element wartet darauf, gesendet zu werden.
- **Gesendet:** Das Element wurde gesendet.
- **In Arbeit:** Der Zielcore ist dabei, das Element zu verarbeiten.
- **Erfolgreich:** Das Element wurde erfolgreich synchronisiert.
- **Fehlgeschlagen:** Das Element konnte nicht erfolgreich synchronisiert werden.

Konfliktmanagement bei der Coresynchronisierung

Exportierbare Elemente der Coresynchronisierung besitzen eine eindeutige Kennung, anhand derer Management Suite verfolgen kann, ob Elemente identisch sind oder nicht. Die Synchronisierungsfunktion kann dadurch Konflikte bei der Synchronisierung von Elementen leichter verwalten. Wenn Sie ein Element auf einen Server kopieren oder synchronisieren und dasselbe Element ist auf dem Zielserver bereits vorhanden, so wird das Element nur dann überschrieben, wenn es dieselbe eindeutige Kennung aufweist. Diese eindeutige Kennung besteht aus dem Namen des Coreservers und der Nummer der Datenbankzeile, die dieses Element enthält. Sie können die eindeutige Kennung und Revisionsnummer eines Elements im Dialogfeld mit Informationen über das Element anzeigen. (klicken Sie mit der rechten Maustaste auf das Element und wählen Sie **Info** aus.)

Wenn zwei Elemente mit demselben Namen unterschiedliche Kennungen aufweisen, dann rührt die Synchronisierung das Original auf dem Ziel nicht an und fügt "%1" zum Dateinamen des synchronisierten Elements hinzu. Die Synchronisierungsfunktion erstellt bei weiteren Synchronisierungskonflikten weiter neue Einträge und setzt diese Nummer jedes Mal um den Wert 1 herauf, bis das Limit von 99 erreicht ist.

Ändern der Einstellungen für die automatische Synchronisierung

Das Intervall für die automatische Synchronisierung des Coreservers ist konfigurierbar. Das Standardintervall beträgt zwei Minuten. Wenn das von Ihnen gewählte Zeitintervall verstrichen ist, prüft der Coreserver die zur automatischen Synchronisierung markierten Elemente auf Änderungen. Wenn sie sich geändert haben, sendet der Core diese Änderungen an die von Ihnen definierten Zielcores. Je nach Größe der Datenmenge, die synchronisiert wird, kann durch ein Verkürzen dieses Intervalls die Prozessorbelastung beim Quellcore geringfügig zunehmen.

Das Dialogfeld "Einstellungen für die automatische Synchronisierung" bietet die folgenden Optionen:

- **Synchronisieren alle:** Das von Ihnen gewünschte Synchronisierungsintervall. Das Standardintervall beträgt zwei Minuten.
- **Maximale Anzahl von Wiederholungsversuchen:** Wie oft dieser Core versuchen wird, eine Verbindung zu den Zielcores herzustellen. Der Standardwert ist fünf. Sobald dieser Grenzwert erreicht ist, unterlässt der Quellcore jeden weiteren Versuch, das Element zu synchronisieren.
- **Daten beim Senden komprimieren:** Die Coresynchronisierung erfolgt über HTTPS. Wenn Sie diese Option aktivieren, wird der Datenstrom außerdem noch komprimiert. Der Standard ist "aktiviert".

- **Schreibschutzwarnung anzeigen, wenn ein Benutzer versucht, automatisch synchronisierte Elemente zu bearbeiten:** Diese Option gilt nur für den Server, auf dem Sie diese Änderung vornehmen und bezieht sich auf automatisch synchronisierte Elemente, die dieser Server empfängt, aber nicht auf Elemente, die von ihm stammen. Sie können diese Option deaktivieren, wenn Sie nicht möchten, dass Konsolenbenutzer eine zusätzliche Warnung erhalten, wenn Sie versuchen, Änderungen an einem automatisch synchronisierten Element auf diesem Server vorzunehmen. Durch Abwählen dieser Option wird lediglich die zusätzliche Warnung deaktiviert. Die Konsolenbenutzer können deshalb trotzdem keinerlei Änderungen an automatisch synchronisierten Elementen vornehmen, die dieser Server empfängt.

So ändern Sie die Einstellungen für die automatische Synchronisierung

1. Klicken Sie auf **Extras > Administration > Coresynchronisierung**.
2. Klicken Sie in der Symbolleiste des Extras **Coresynchronisierung** auf die Schaltfläche **Einstellungen für automatische Synchronisierungsdienste bearbeiten**.
3. Geben Sie das von Ihnen gewünschte Synchronisierungsintervall ein.
4. Ändern Sie bei Bedarf die Einstellungen der anderen Optionen.
5. Klicken Sie auf **OK**.

So starten Sie die Synchronisierung bei einem Element neu, bei dem das Limit für Wiederholversuche überschritten wurde

1. Klicken Sie auf **Extras > Administration > Coresynchronisierung**.
2. Klicken Sie unter **Coreserver** auf den Server, auf dem Sie die Synchronisierung neu starten möchten.
3. Klicken Sie im Protokoll auf das Element, bei dem die Synchronisierung fehlgeschlagen ist, und wählen Sie **Erneut synchronisieren** aus.

Agentenkonfiguration

Konfigurieren von Geräteagenten

Damit Geräte vollständig verwaltbar sind, müssen die Management Suite Agenten auf ihnen installiert sein. Dieses Kapitel befasst sich mit folgenden Themen:

- "Verwenden von Agentenkonfigurationen" auf Seite 107
- "Erstellen einer Agentenkonfiguration" auf Seite 108
- "Verwenden des Advance Agent" auf Seite 110
- "Aktualisieren von Agenteneinstellungen auf Geräten" auf Seite 113
- "Erstellen eines Standalone-Agentenkonfigurationspakets" auf Seite 113
- "Agentensicherheit und vertrauenswürdige Zertifikate" auf Seite 114
- "Deinstallieren von Geräteagenten" auf Seite 118

Mit dem Fenster **Agentenkonfiguration** können Sie neue Agentenkonfigurationen für Ihre Windows-, Linux- und Macintosh-Geräte definieren. Die von Ihnen erstellten Agentenkonfigurationen können anschließend über das Konsolenfenster **Geplante Tasks** an Clients übertragen werden.

HINWEIS: Agentenbereitstellung auf Windows 95/98/NT-Geräten
Management Suite wird ab sofort nicht mehr mit Agenten geliefert, die Windows 95-, Windows 98- oder Windows NT-Geräte unterstützen. Sollten Sie den Legacy-Agenten benötigen, der auf diesen Geräten funktioniert, wenden Sie sich bitte an den LANDesk Kundendienst.

HINWEIS: Gerätekonfigurationen für Windows-Geräte erstellen, die nicht für die Verwaltung aktiviert sind
Wenn Sie über Windows -Geräte verfügen, die Teil einer Windows-Domäne sind, können Sie per "Push"-Vorgang auch dann eine Konfiguration an diese Geräte übertragen, wenn der Standard LANDesk Agent und die Remotesteuerungsagenten nicht installiert sind. Weitere Informationen finden Sie in der Dokumentation zur Bereitstellung auf der Website der LANDesk Community unter http://community.landesk.com.

HINWEIS: Agentenkonfiguration in Umgebungen mit unterschiedlichen Sprachversionen
Wenn Sie Agentenkonfigurationen in Umgebungen mit unterschiedlichen Sprachversionen erstellen, müssen Sie sicherstellen, dass der Agentenkonfigurationsname nur ASCII-Zeichen aufweist (d. h. nur Zeichen des englischen Zeichensatzes). Ein englischer Coreserver ist mit allen unterstützten Sprachen kompatibel. Wenn jedoch in einem Agentenkonfigurationsnamen Nicht-ASCII-Zeichen verwendet werden, wie etwa japanische, chinesische oder russische Zeichen, so muss die Agentenkonfiguration auf einem Core bzw. einer Konsole mit genau dieser Sprache erstellt werden und sie funktioniert dann auch nur auf Geräten mit derselben Sprache. Eine Agentenkonfiguration, die japanische Zeichen enthält, muss beispielsweise auf einem japanischen Core erstellt werden und dann auch auf einem japanischen Client bereitgestellt werden.

Konfigurieren der Agentenerkennung

Der Begriff "Agentenerkennung" bezeichnet das Verfahren, mit dem verwaltete Geräte ausfindig gemacht werden, auf denen der Standard LANDesk Agent oder Remotesteuerungsagent installiert ist. Diese beiden Agenten stellen folgende Funktionen zur Verfügung:

- **Standard LANDesk Agent:** Aktiviert den Ping Discovery Service (PDS). Wenn der Standard LANDesk Agent auf einem Gerät installiert ist, können Sie Softwareverteilungen und Gerätesetup-Konfigurationen planen.
- **Remotesteuerung:** Gibt Ihnen die Möglichkeit per Remotezugriff auf ein Gerät zuzugreifen und es zu steuern.

Die Agentenerkennung verwendet TCP/IP, um Agenten zu überprüfen, die auf den Geräten ausgeführt werden.

IP-Adressen werden als Suchkriterien verwendet, um eine Standard LANDesk Agent-Erkennung mit TCP/IP durchzuführen. Management Suite sucht auf Geräten in einem bestimmten IP-Adressbereich nach dem Standard Management Suite Agenten und dem Remotesteuerungsagenten. Dieser Adressbereich wird durch die von Ihnen angegebene IP-Netzwerkadresse vorgegeben.

Wenn Sie keine Subnetz-Netzwerkadressen bei der TCP/IP-Suche designieren, wird die Erkennung nur in dem Netzwerksegment durchgeführt, in dem die Konsole, die die Erkennung initiiert, resident ist. Wenn Sie z. B. vier Konsolen installiert haben, von denen jede in einem anderen Netzwerksegment resident ist, müssten Sie vier Scans initiieren – einen von jeder der vier Konsolen aus.

In Netzwerksegmenten, in denen es keine Konsolen gibt, müssen Sie Subnetz-Netzwerkadressen verwenden, um auf die Daten dieses Netzwerksegments zuzugreifen.

HINWEIS: Wenn in Ihrem Netzwerk Firewalls installiert sind, kann die Agentenerkennung nicht zum Suchen außerhalb der Firewall(s) verwendet werden, da Firewalls im Allgemeinen den Fluss der Paketdaten an designierte Anschlüsse begrenzen.

Die Agentenerkennung führt standardmäßig nur für das ausgewählte Gerät eine Erkennung durch. Sie können die Erkennungsoptionen anpassen, indem Sie die nachstehend beschriebenen Schritte ausführen.

So konfigurieren Sie Optionen für die Agentenerkennung

1. Klicken Sie auf **Konfigurieren** > **Optionen für den Agentenstatus**.
2. Wählen Sie die gewünschten Erkennungs- und Aktualisierungsoptionen aus. Nähere Informationen hierzu finden Sie im nächsten Abschnitt.
3. Klicken Sie auf **OK**.

Informationen zum Dialogfeld "Optionen für den Agentenstatus"

In diesem Dialogfeld können Sie folgende Erkennungsoptionen konfigurieren:

- **Agentenstatus erfassen:**
  - **Nie:** Den Agentenstatus nie erfassen. Diese Option verwenden Sie, wenn eine große Zahl unzuverlässiger Geräte oder eine langsame Netzwerkverbindung vorliegt.
  - **Nur für ausgewählte sichtbare Elemente:** Legt fest, dass der Agentenstatus eines Geräts aktualisiert wird, wenn das Gerät in der Netzwerkansicht ausgewählt wird. Sie sollten diese Option verwenden und die automatische Aktualisierung deaktivieren, wenn das Verhältnis der verfügbaren Geräte zu den nicht verfügbaren Geräte etwa 50/50 beträgt. Der Einsatz dieser Option und die Deaktivierung der automatischen Aktualisierung empfiehlt sich auch, wenn Sie den durch die Konsole erzeugten Netzwerkverkehr reduzieren möchten.

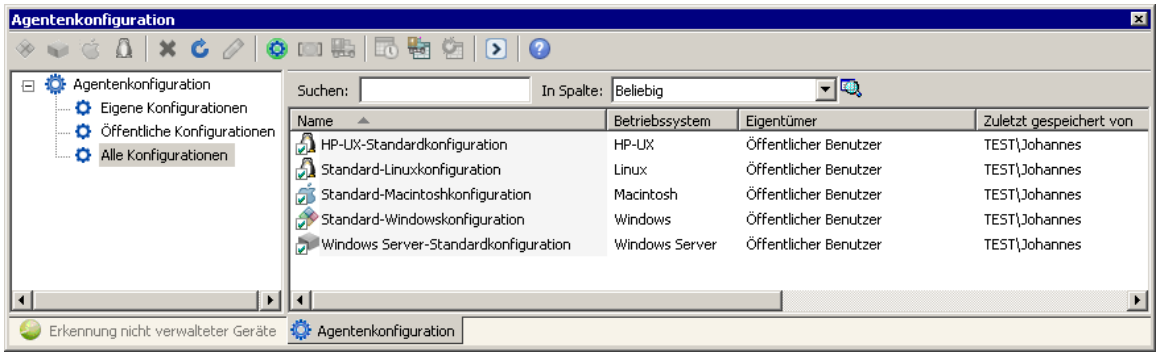
- **Für alle sichtbaren Elemente:** Legt fest, dass für alle sichtbaren Geräte in der Netzwerkansicht der Agentenstatus entsprechend der Aktualisierungsrate aktualisiert wird. Wenn neue Geräte sichtbar werden, wird ihr Agentenstatus (und Zustand) aktualisiert. Diese Option verursacht den meisten Netzwerkverkehr.

- **Aktualisierung alle < > Minuten:** Gibt an, ob der Agentenstatus automatisch in dem von Ihnen gewählten Zeitintervall aktualisiert wird. Zur Aktivierung dieser Option markieren Sie das Kästchen neben **Aktualisieren**. Diese Option ist standardmäßig deaktiviert und das Aktualisierungsintervall kommt nur zur Anwendung, wenn das Kontrollkästchen der Option aktiviert wird. Wenn Sie diese Option aktivieren, sollten Sie entweder das standardmäßige 5-Minuten-Intervall oder ein längeres Intervall verwenden, um den Netzwerkverkehr möglichst gering zu halten.

Verwenden von Agentenkonfigurationen

Management Suite verwendet Agentenkonfigurationen, mit denen Sie Agenten und Agenteneinstellungen auf verwalteten Geräten bereitstellen können. Sobald die Management Suite-Agenten auf den Geräten installiert sind, lassen sich Agentenkonfigurationen problemlos aktualisieren.

Das Extra "Agentenkonfiguration" verwenden Sie, um Geräte- und Serverkonfigurationen zu erstellen und zu aktualisieren (beispielsweise, welche Agenten auf Geräten installiert sind und welche Netzwerkprotokolle die Agenten verwenden usw.). Sie können verschiedene Konfigurationen erstellen, die auf den spezifischen Bedarf einer Abteilung oder Gruppe zugeschnitten sind. So können Sie beispielsweise Konfigurationen für die Geräte in der Buchhaltung oder für Geräte mit einem bestimmten Betriebssystem erstellen. Für jeden Konfigurationstyp kann es immer nur eine Standardkonfiguration geben. Die Standardkonfiguration kann zwar nicht gelöscht, aber bearbeitet werden. Sie sollten es nach Möglichkeit vermeiden, zu viele verschiedene Konfigurationen zu erstellen, da dies den Support und die Fehlerbehebung komplizierter und aufwändiger macht.



Vor der Installation einer Agentensoftware muss zunächst eine Agentenkonfiguration erstellt werden (oder es muss die Standardkonfiguration verwendet werden). Dies erfordert einigen Planungs- und Testaufwand. Eine bereitgestellte Konfiguration sollte idealerweise von Anfang an fehlerfrei sein – auch wenn eine Neukonfiguration und erneute Bereitstellung des Agenten möglich ist.

Eine Organisation benötigt unter Umständen mehrere verschiedene Agentenkonfigurationen. Ein Laptopcomputer zum Beispiel erfordert unter Umständen eine andere Konfiguration als ein Desktopsystem. Um zu vermeiden, dass der falsche Agent für ein System bereitgestellt wird, ist es wichtig, vernünftige Namenskonventionen für alle Agentenkonfigurationen zu definieren und einzuhalten.

Der Sicherheits- und Patchscanner-Agent wird standardmäßig mit dem Standard LANDesk Agent installiert. Sie können Sicherheitsscans konfigurieren, um festzulegen, wie und wann der Sicherheitsscanner auf verwalteten Geräten ausgeführt und ob der Scanverlauf sowie interaktive Optionen auf dem Gerät des Endanwenders angezeigt werden. (Mit dem Sicherheitsscanner können Sie nach LANDesk Software-Updates auf Geräten und Coreservern suchen, selbst wenn Sie kein Inhaltsabonnement für LANDesk Security Suite besitzen. Mit einem Security Suite-Abonnement können Sie die gesamte Kapazität des Sicherheitsscanners nutzen, um bekannte Anfälligkeiten, Spyware, unzulässige Anwendungen, Viren und andere potenzielle Sicherheitsrisiken ausfindig machen und reparieren).

Lesen Sie unbedingt die Informationen zu den bekanntesten Methoden der Agentenbereitstellung, die Sie auf der Website der LANDesk Benutzercommunity unter http://community.landesk.com/support/docs/DOC-23482 finden.

WICHTIG: Wenn Sie Agentenkonfigurationen in Umgebungen mit unterschiedlichen Sprachversionen erstellen, müssen Sie sicherstellen, dass der Agentenkonfigurationsname nur ASCII-Zeichen aufweist (d. h. nur Zeichen des englischen Zeichensatzes). Ein englischer Coreserver ist mit Clients in allen unterstützten Sprachen kompatibel.

Wenn jedoch in einem Agentenkonfigurationsnamen Nicht-ASCII-Zeichen verwendet werden, wie etwa japanische, chinesische oder russische Zeichen, so muss die Agentenkonfiguration auf einem Core bzw. einer Konsole mit genau dieser Sprache erstellt werden und sie funktioniert dann auch nur auf Geräten mit derselben Sprache. Eine Agentenkonfiguration, die japanische Zeichen enthält, muss beispielsweise auf einem japanischen Core erstellt werden und dann auch auf einem japanischen Client bereitgestellt werden.

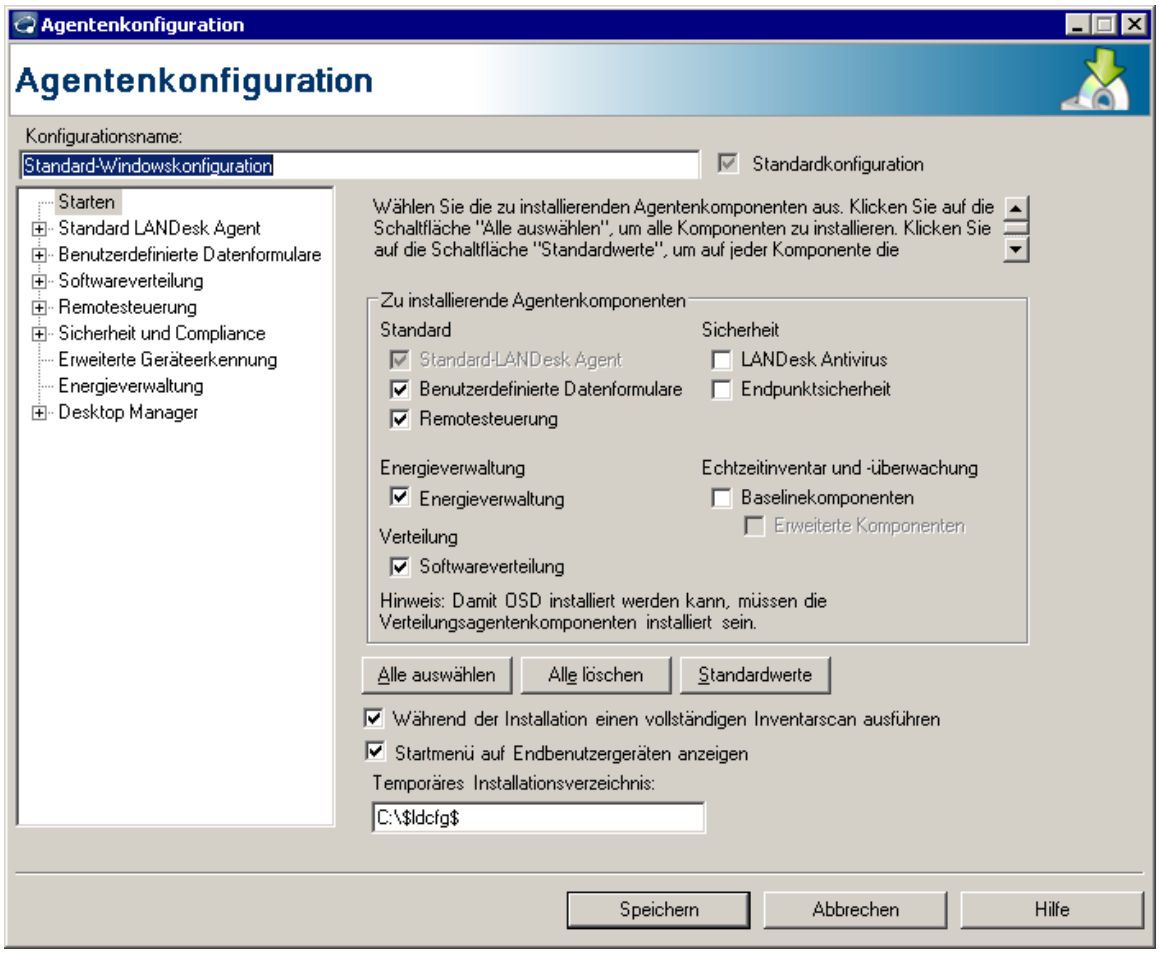
Lesen Sie die nachstehenden Abschnitte, um mehr über folgende Themen zu erfahren:

- "Erstellen einer Agentenkonfiguration" auf Seite 108
- "Verwenden des Advance Agent" auf Seite 110
- "Aktualisieren von Agenteneinstellungen auf Geräten" auf Seite 113

Erstellen einer Agentenkonfiguration

Verwenden Sie das Fenster **Agentenkonfiguration**, um Geräte- und Serverkonfigurationen zu erstellen und zu aktualisieren (beispielsweise, welche Agenten auf Geräten installiert sind und welche Netzwerkprotokolle die Agenten verwenden usw.).

Sie können verschiedene Konfigurationen erstellen, die auf den jeweiligen Bedarf spezifischer Gruppen zugeschnitten sind. Sie können beispielsweise Konfigurationen für die Geräte in der Buchhaltung oder für Geräte mit einem bestimmten Betriebssystem erstellen.



Um eine Konfiguration auf Geräte zu übertragen, müssen Sie folgende Schritte ausführen:

- **Die Agentenkonfiguration erstellen:** Definieren Sie spezifische Konfigurationen für Ihre Geräte. Eine "Advance Agent Konfiguration" ist in der Regel die beste Wahl. Nähere Informationen hierzu finden Sie im nächsten Abschnitt unter "Verwenden des Advance Agent" auf Seite 110.
- **Agentenkonfiguration planen:** Übertragen Sie die Konfiguration mit einem Pushvorgang auf Geräte, auf denen der Standard LANDesk Agent installiert ist. Benutzer mit administrativen Rechten können außerdem die Standardagentenkonfiguration installieren, indem Sie wscfg32.exe oder IPSETUP.BAT aus der LDLogon-Freigabe des Coreservers ausführen.

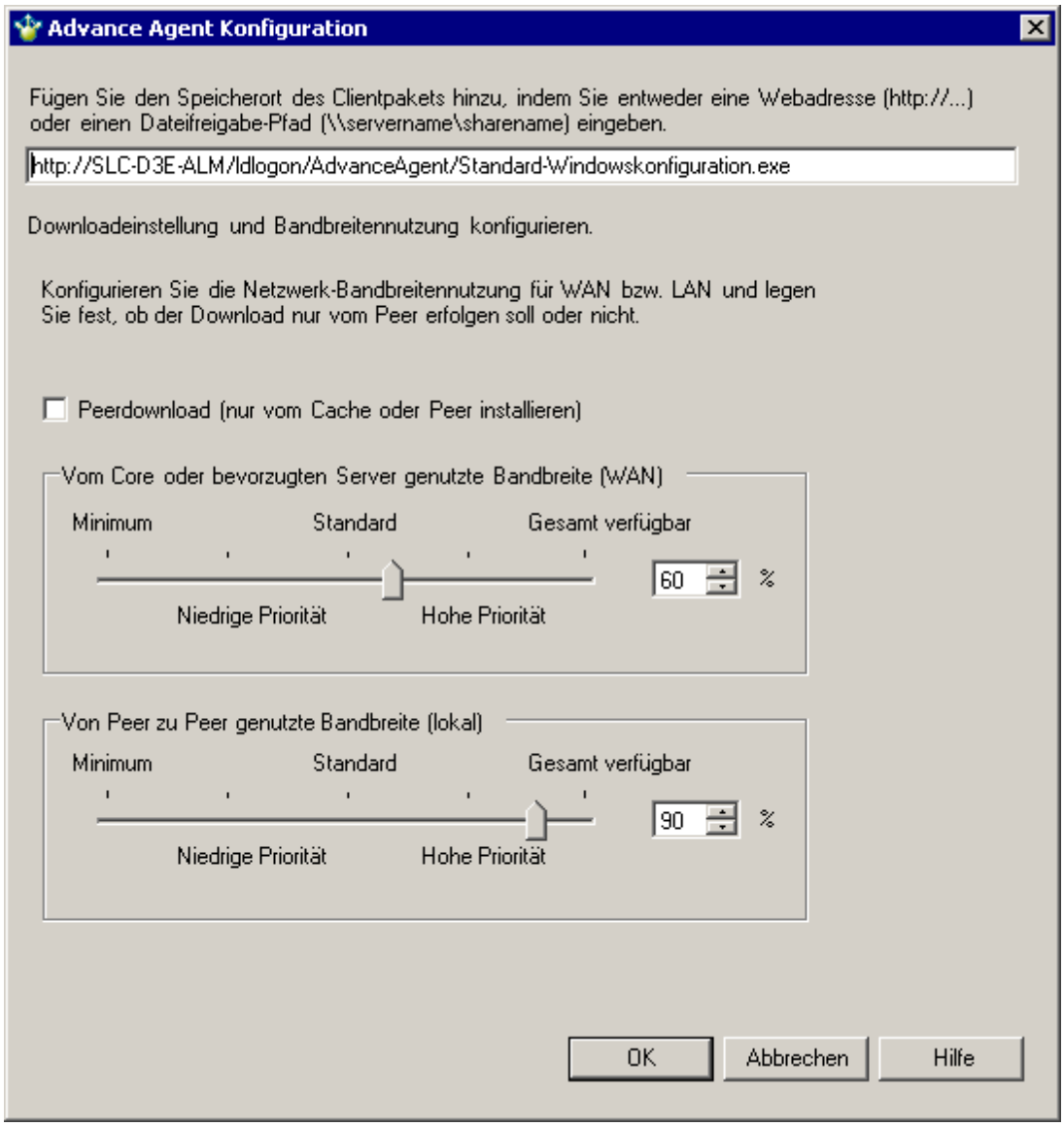
So erstellen Sie eine Agentenkonfiguration

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie im Baum **Agentenkonfiguration** auf die gewünschte Konfigurationskategorie.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neues Windows, Neuer Windows-Server, Neuer Macintosh** oder **Neue Linux-Konfiguration**.
4. Geben Sie einen **Konfigurationsnamen** ein.
5. Wählen Sie auf der **Startseite** des Fensters **Agentenkonfiguration** die Agenten aus, die Sie bereitstellen möchten.

6. Navigieren Sie mithilfe der Strukturansicht in den Dialogfeldern, die sich auf die von Ihnen ausgewählten Optionen beziehen. Passen Sie die von Ihnen ausgewählten Optionen nach Bedarf an. Klicken Sie auf **Hilfe**, um weitere Informationen anzuzeigen, wenn Sie Fragen zu einer Seite haben.
7. Klicken Sie auf **Speichern**.
8. Wenn Sie die Konfiguration als Standard, d. h. als die Konfiguration, die von ldlogon\wscfg32.exe oder ldlogon\IPSETUP.BAT installiert wird, einrichten möchten, klicken Sie im Kontextmenü der Konfiguration auf **Standardkonfiguration**.

Verwenden des Advance Agent

Für die Mehrzahl der Umgebungen stellt der Advance Agent die bevorzugte Methode für die Bereitstellung des Agenten dar. Dieser Agent wurde erstellt, um die bandbreitenfreundliche LANDesk Technologie auch bei der Agentenbereitstellung nutzen zu können. Mit ihm können Sie die Netzwerkbandbreite reduzieren, die für die Windows-basierte Agentenkonfiguration verwendet wird. Der Advance Agent verwendet ein zweistufiges Bereitstellungsverfahren. Beim Advance Agent handelt es sich um eine MSI-Datei, die vor dem vollständigen Agenten bereitgestellt wird. Die MSI-Datei wird installiert und initiiert dann den Download und die Installation des vollständigen Agentenpakets.



Der Advance Agent ist für die meisten Geräte geeignet einschließlich Laptops mit intermittierenden oder langsamen Netzwerkverbindungen. PDAs und andere Handheld-Geräte werden jedoch von diesem Agenten nicht unterstützt.

Der Advance Agent ist ein kleines MSI-Paket mit 500 KB. Wenn Sie dieses Paket auf einem verwalteten Gerät ausführen, lädt es ein zugehöriges Konfigurationspaket für einen vollständigen Agenten. Je nachdem, welche Agenten Sie auswählen, kann dieses Paket eine Größe von bis zu 15 MB erreichen. Im Dialogfeld **Advance Agent Konfiguration** können Sie bandbreitenfreundliche Verteilungsoptionen konfigurieren, die dann beim Download der Konfiguration für den vollständigen Agenten von MSI verwendet wird.

Sobald der Advance Agent beginnt, die Konfiguration für den vollständigen Agent downzuloaden, arbeitet er unabhängig vom Coreserver. Wenn die Verbindung des Geräts mit dem Netzwerk getrennt wird, bevor die Agentenkonfiguration vollständig heruntergeladen werden konnte, setzt der Advance Agent den Downloadvorgang automatisch fort, sobald das Gerät wieder mit dem Netzwerk verbunden ist.

Beim Erstellen einer einer Advance Agent-Konfiguration dauert es einige Sekunden, bis die Konsole das Konfigurationspaket für den vollständigen Agent erstellt hat. Die Konsole fügt das Advance Agent-Paket (<Konfigurationsname>.msi) und das neu erstellte Konfigurationspaket für den vollständigen Agent (<Konfigurationsname>.exe) in den Ordner "LDLogon\AdvanceAgent" des Coreservers ein. Die Dateinamen leiten sich aus dem Namen der Agentenkonfiguration ab.

Sobald Sie ein Agenten-Konfigurationspaket erstellt haben, müssen Sie den MSI-Teil mit einer der folgenden Methoden ausführen:

- Eine Pushverteilung des kleinen MSI-Teils planen.
- Den MSI auf jedem Gerät manuell ausführen.
- Den MSI manuell für die Ausführung über ein Anmeldeskript konfigurieren.

Sobald Sie den Advance Agent auf Geräten bereitstellen, beginnt dieser, die entsprechende Agentenkonfiguration downzuloaden. Der Agent wird im Hintergrund auf dem verwalteten Gerät ausgeführt, d. h., es werden weder Dialogfelder noch Statusinformationen eingeblendet. Der Advance Agent verwendet die Bandbreiteneinstellungen, die Sie im Dialogfeld **Advance Agent Konfiguration** festgelegt haben, beispielsweise Peerdownload und dynamische Bandbreitendrosselung.

Sobald der MSI installiert ist und begonnen hat, Agenten auf einem Gerät zu konfigurieren, entfernt er das Konfigurationspaket für den vollständigen Agenten. Der MSI-Teil verbleibt auf dem Gerät, und wenn derselbe MSI erneut ausgeführt wird, installiert dieser nicht die Agenten neu.

Erstellen einer Advance Agent-Konfiguration

So definieren Sie eine Advance Agent-Konfiguration

1. Erstellen Sie eine Windows-basierte Agentenkonfiguration (**Extras > Konfiguration > Agentenkonfiguration**).
2. Klicken Sie im Kontextmenü der Konfiguration auf **Advance Agent**.
3. Wählen Sie die gewünschten Optionen aus.
4. Wenn Sie **Peerdownload** auswählen, müssen Sie darauf achten, dass sich die .msi-Datei des Advance Agent und das gesamte .exe-Paket der Agentenkonfiguration im Cache der Softwareverteilung eines Geräts in der Broadcast-Domäne befinden. Wenn Sie **Peerdownload** auswählen und dies vor dem Bereitstellen der Advance Agent-Konfiguration nicht tun, schlägt die Bereitstellung fehl, weil kein Cache oder Peer in der Broadcast-Domäne über die nötigen Dateien verfügt.
5. Wenn Sie planen, das zugehörige Agent-Konfigurationspaket (die .exe-Datei) in einen anderen Speicherort zu verschieben, ändern Sie den Pfad für das Agenten-Konfigurationspaket, damit er dem geänderten Speicherort entspricht.
6. Klicken Sie auf **OK**.
7. Kopieren Sie ggf. die zugehörige .exe-Datei aus dem Ordner "LDLogon\AdvanceAgent" auf Ihren Verteilungsserver. Stellen Sie sicher, dass der Pfad zur ausführbaren Datei der Agentenkonfiguration mit dem Pfad übereinstimmt, den Sie im Dialogfeld **Advance Agent Konfiguration** angegeben hatten. Sie sollten das MSI-Paket im Standardspeicherort auf dem Coreserver belassen. Wenn Sie das Paket verschieben, ist es für den unten beschriebenen Advance Agent Pushverteilungstask nicht mehr sichtbar.

So konfigurieren Sie eine Pushverteilung für den Advance Agent

1. Klicken Sie im Fenster "Agentenkonfiguration" (**Extras > Konfiguration > Agentenkonfiguration**) auf die Schaltfläche **Pushverteilung einer Advance Agent-Konfiguration planen**.
2. Im Dialogfeld **Advance Agent Konfigurationen** werden die Agentenkonfigurationen aufgelistet, die im Ordner "LDLogon\AdvanceAgent" gespeichert sind. Klicken Sie auf die Konfiguration, die Sie verteilen möchten, und klicken Sie auf **OK**.
3. Das Fenster **Geplante Tasks** wird geöffnet. Der von Ihnen erstellte Advance Agent-Task ist darin bereits ausgewählt. Der Taskname ist "Advance Agent <Ihr Konfigurationsname>".
4. Fügen Sie Zielgeräte zum Task hinzu, indem Sie die entsprechenden Geräte aus der Netzwerkansicht ziehen und auf dem Task im Fenster **Geplante Tasks** ablegen.
5. Klicken Sie im Kontextmenü des Tasks auf **Eigenschaften** und planen Sie den Task. Der Status der MSI-Verteilung lässt sich im Fenster **Geplante Tasks** verfolgen. Nach Abschluss der MSI-Verteilung gibt es keine Statusupdates zur Konfiguration des vollständigen Agent.

Aktualisieren von Agenteneinstellungen auf Geräten

Wenn Sie Agenteneinstellungen auf Geräten aktualisieren möchten (beispielsweise das Abfragen eines Berechtigungsnachweises für die Remotesteuerung), müssen Sie nicht die gesamte Agentenkonfiguration neu bereitstellen. Sie können die gewünschten Änderungen im Fenster **Agentenkonfiguration** vornehmen und im Kontextmenü dieser Konfiguration auf **Update planen** klicken. Hiermit wird das Fenster **Geplante Tasks** geöffnet und ein Aktualisierungstask und -paket für die Konfiguration, mit der Sie die Aktualisierung geplant haben, erstellt. Diese Paket ist nur wenige Hundert Kilobyte groß.

Beim Aktualisieren von Einstellungen werden keine Agenten auf einem Gerät installiert oder entfernt. Wenn die Aktualisierung Einstellungen für Agenten enthält, die sich nicht auf dem betreffenden Gerät befinden, werden die nicht relevanten Einstellungen ignoriert.

WICHTIG: Die Agentenüberwachung bietet keine Unterstützung für die Änderung von Einstellungen durch geplante Updates. Wenn Sie Einstellungen der Agentenüberwachung ändern möchten, klicken Sie mit der rechten Maustaste in der Netzwerkansicht auf das gewünschte Gerät und klicken Sie dann auf **Agentenüberwachungseinstellungen aktualisieren**.

So aktualisieren Sie Agenteneinstellungen auf Geräten

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Passen Sie die Konfiguration an, die Sie verwenden möchten.
3. Klicken Sie nach Abschluss dieses Vorgangs im Kontextmenü der Konfiguration auf **Agenteneinstellungs-Update planen**. Das Fenster **Geplante Tasks** wird geöffnet.
4. Wählen Sie die Geräte aus, die Sie aktualisieren möchten, und planen Sie den Task.

Erstellen eines Standalone-Agentenkonfigurationspakets

Normalerweise werden Clients vom Client-Konfigurationstool wscfg32.exe konfiguriert. Sie haben jedoch auch die Möglichkeit, im Fenster **Agentenkonfiguration** eine selbstextrahierende ausführbare Datei erstellen zu lassen, die eine Agentenkonfiguration auf dem Gerät installiert, auf dem sie ausgeführt wird. Dies ist nützlich, wenn Sie Agenten von einer CD- oder einem mobilem USB-Laufwerk installieren oder eine Agentenkonfiguration mit Multicasting verteilen möchten.

So erstellen Sie ein eigenständiges Agenten-Konfigurationspaket

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Passen Sie die Konfiguration an, die Sie verwenden möchten.
3. Klicken Sie nach Abschluss dieses Vorgangs im Kontextmenü der Konfiguration auf **Unabhängiges Clientinstallationspaket erstellen**.
4. Wählen Sie den Pfad aus, in dem das Paket gespeichert werden soll. Stellen Sie sicher, dass der Dateiname ausschließlich ASCII-Zeichen (a bis z, A bis Z, 0 bis 9) enthält.
5. Warten Sie, bis Management Suite das Paket erstellt hat. Dieser Vorgang kann mehrere Minuten in Anspruch nehmen.

Agentensicherheit und vertrauenswürdige Zertifikate

Management Suite 8 verwendet ein zertifikatbasiertes Authentifizierungssystem. Geräteagenten werden durch autorisierte Coreserver authentifiziert, um den nicht autorisierten Zugriff von Cores auf Clients zu verhindern. Jeder Coreserver verfügt über ein eindeutiges Zertifikat und einen privaten Schlüssel, das/der von Management Suite-Setup beim erstmaligen Installieren des Coreservers oder Rollup-Coreservers erstellt wird.

Dies sind die privaten Schlüssel- und Zertifikatdateien:

- **<Schlüsselname>.key:** Die .key-Datei ist der private Schlüssel für den Coreserver und ist nur auf dem Coreserver vorhanden. Wenn dieser Schlüssel nicht mehr intakt ist, sind Coreserver und die Gerätekommunikation nicht mehr sicher. Achten Sie auf die Sicherheit dieses Schlüssels. Senden Sie ihn beispielsweise nicht per E-Mail.
- **<Schlüsselname>.crt:** Die .crt-Datei enthält den öffentlichen Schlüssel für den Coreserver. Die .crt-Datei ist eine Version des öffentlichen Schlüssels, die sich leichter anzeigen lässt, um weitere Informationen über den Schlüssel zu erhalten.
- **<hash>.0:** Die .0-Datei ist eine vertrauenswürdige Zertifikatdatei, deren Inhalt mit der .crt-Datei identisch ist. Ihr Name wird jedoch so gewählt, dass der Computer die Zertifikatdatei in einem Ordner, der viele verschiedene Zertifikate enthält, schnell findet. Der Name ist ein Hash (Prüfsumme) der Subjektinformationen des Zertifikats. Um den Hash-Dateinamen eines bestimmten Zertifikats zu bestimmen, zeigen Sie die <Schlüsselname>.crt-Datei an. Die Datei enthält einen .ini-Dateiabschnitt [LDMS]. Das Hash=Wert-Paar gibt den <Hash>-Wert an.

Alternativ kann der Hash-Wert auch mithilfe der Anwendung "openssl" bestimmt werden, die im Ordner \Programme\LANDesk\Shared Files\Keys gespeichert ist. Sie zeigt mithilfe der folgenden Befehlszeile den mit einem Zertifikat assoziierten Hash-Wert an:

```
openssl.exe x509 -in <Schlüsselname>.crt -hash -noout
```

Alle Schlüssel sind auf dem Coreserver gespeichert unter \Programme\LANDesk\Shared Files\Keys. Der öffentliche <hash>.0 Schlüssel befindet sich ebenfalls im ldlogon-Ordner und muss dort standardmäßig abgelegt sein. <Schlüsselname> ist der Zertifikatname, der von Ihnen während des Setups von Management Suite angegeben wurde. Während des Setups ist es hilfreich, einen beschreibenden Schlüsselnamen anzugeben, z. B. den Namen des Coreservers (oder sogar dessen vollständig qualifizierten Namen) (Beispiel: ldcore oder ldcore.org.com). Dies vereinfacht die Identifizierung des Zertifikats/des privaten Schlüssels in einer Umgebung mit mehreren Cores.

Sie sollten vom Inhalt des Schlüsselordners Ihres Coreservers eine Sicherungskopie anlegen und diese sicher aufbewahren. Wenn Sie den Coreserver neu installieren oder austauschen müssen, können Sie die Geräte des betreffenden Coreservers so lange nicht verwalten, bis Sie die Zertifikate des ursprünglichen Cores wie unten beschrieben zum neuen Core hinzugefügt haben.

Gemeinsame Nutzung von Schlüsseln unter Coreservern

Geräte kommunizieren nur mit Coreservern und Rollup-Coreservern, für die sie eine übereinstimmende Datei für ein vertrauenswürdiges Zertifikat haben. Angenommen, Sie verfügen über drei Coreserver, von denen jeder 5.000 Geräte verwaltet. Außerdem setzen Sie einen Rollup-Coreserver für die Verwaltung aller 15.000 Geräte ein. Jeder Coreserver hat ein eigenes Zertifikat und private Schlüssel. Zudem kommunizieren die Geräteagenten, die Sie von dem jeweiligen Coreserver aus bereitstellen, standardmäßig nur mit dem Coreserver, von dem aus die Gerätesoftware bereitgestellt wird.

Es gibt zwei Hauptmethoden für die gemeinsame Schlüsselnutzung von Coreservern und Rollup-Coreservern:

1. Verteilung des vertrauenswürdigen Zertifikats eines jeden Coreservers (Datei "<hash>.0") an Geräte und ihre entsprechenden Coreserver. Dies ist die sicherste Methode.
2. Kopieren des privaten Schlüssels und der Zertifikate auf die einzelnen Coreserver. Auf den Geräten müssen hierfür keine Änderungen vorgenommen werden. Da Sie jedoch den privaten Schlüssel kopieren müssen, ist das Risiko größer.

Wenn Sie in diesem Beispiel möchten, dass der Rollup-Core und die Webkonsole Geräte von allen drei Cores verwalten, müssen Sie das vertrauenswürdige Zertifikat des Rollup-Cores (Datei "<hash>.0") auf alle Geräte verteilen und dieselbe Datei in den Idlogon-Ordner eine jeden Coreservers kopieren. Nähere Informationen hierzu finden Sie im nächsten Abschnitt. Alternativ können Sie auch das Zertifikat/den privaten Schlüssel von jedem der drei Coreserver auf den Rollup-Core kopieren. Auf diese Weise findet jedes Gerät den passenden privaten Schlüssel für seinen Coreserver auf dem Rollup-Coreserver. Weitere Informationen finden Sie unter "Kopieren von Dateien für Zertifikate/private Schlüssel von Coreserver nach Coreserver" auf Seite 116.

Wenn ein Core Geräte eines anderen Cores verwalten soll, können Sie dasselbe Verfahren anwenden und entweder das vertrauenswürdige Zertifikat auf Geräte verteilen oder die Datei des Zertifikats/öffentlichen Schlüssels unter den Cores verteilen.

Wenn Sie Zertifikate unter eigenständigen Coreservern (keine Rollup-Cores) kopieren, kommt noch folgendes Problem hinzu. Ein Core ist nicht in der Lage, die Geräte eines anderen Core zu verwalten, es sei denn, er erhält vorab Zugriff auf einen Inventarscan der betreffenden Geräte. Eine Möglichkeit, Inventarscans auf einen anderen Core zu übertragen, besteht darin, einen Auftrag für einen Inventarscan zu planen, der den Scan mithilfe einer benutzerdefinierten Befehlszeile an den neuen Core weiterleitet. In einer Konfiguration mit mehreren Coreservern ist die Verwendung eines Rollup-Cores und der Webkonsole eine einfachere Möglichkeit, Geräte über mehrere Cores hinweg zu verwalten. Rollup-Cores erhalten automatisch Inventarscan-Daten von allen Geräten auf den Cores, für die ein Rollup durchgeführt wird.

Verteilen von vertrauenswürdigen Zertifikaten an Geräte

Es gibt zwei Methoden für die Bereitstellung von vertrauenswürdigen Zertifikaten auf Geräten:

1. Bereitstellen einer Gerätesetup-Konfiguration, die die gewünschten vertrauenswürdigen Zertifikate für Coreserver enthält.

2. Verwenden eines Softwareverteilungsauftrags, um die gewünschten Dateien für das vertrauenswürdige Zertifikat auf jedes Gerät zu kopieren.

Jedes zusätzliche vertrauenswürdige Zertifikat für Coreserver (<hash>.0), das die Geräte verwenden sollen, muss in den ldlogon-Ordner des Coreservers kopiert werden. Sobald sich das vertrauenswürdige Zertifikat in diesem Ordner befindet, können Sie es auf der Seite **Common Base Agent** des Dialogfelds für das Gerätesetup auswählen. Das Gerätesetup kopiert Schlüssel in folgenden Ordner auf den Geräten:

- Windows-Geräte: \Programme\LANDesk\Shared Files\cbaroot\certs
- Mac OS X-Geräte: /usr/LANDesk/common/cbaroot/certs

Wenn Sie das Zertifikat eines Coreservers zu einem Gerät hinzufügen möchten und Sie keine Geräteagenten über das Gerätesetup neu verteilen möchten, erstellen Sie einen Softwareverteilungsauftrag, der < hash>.0 in den oben angegebenen Ordner auf dem Gerät kopiert. Anschließend können Sie dann mit dem Fenster **Geplante Tasks** das von Ihnen erstellte Zertifikatverteilungsskript bereitstellen.

Nachfolgend finden Sie ein Beispiel für ein benutzerdefiniertes Skript, das zum Kopieren eines vertrauenswürdigen Zertifikats aus dem Ordner "ldlogon" des Coreservers auf ein Gerät verwendet werden kann. Ersetzen Sie hierzu "d960e680" mit dem Hash-Wert für das vertrauenswürdige Zertifikat, das Sie bereitstellen möchten.

```
; Kopieren Sie ein vertrauenswürdiges Zertifikat aus dem Verzeichnis ldlogon des Coreservers
; in das Verzeichnis der vertrauenswürdigen Zertifikate des Clients
[MACHINES]
REMCOPY0=%DTMDIR%\ldlogon\d960e680.0, %TRUSTED_CERT_PATH%\d960e680.0
```

Kopieren von Dateien für Zertifikate/private Schlüssel von Coreserver nach Coreserver

Eine Alternative zum Bereitstellen von Zertifikaten (<hash>.0) auf Geräten ist das Kopieren von Zertifikatgruppen bzw. Gruppen mit privaten Schlüsseln von Coreserver nach Coreserver. Cores können mehrere Dateien für Zertifikate/private Schlüssel enthalten. Solange sich ein Agent mit einem der Schlüssel auf einem Core authentifizieren kann, ist die Kommunikation mit diesem Core möglich.

HINWEIS: Bei Verwendung der zertifikatbasierten Remotesteuerung müssen sich die Zielgeräte in der Coredatenbank befinden.
Wenn Sie die zertifikatbasierte Remotesteuerungssicherheit auf Geräten verwenden, lassen sich nur solche Geräte remote steuern, die über einen Inventardatensatz in der Coredatenbank verfügen, mit der Sie verbunden sind. Vor der Kontaktaufnahme mit einem Knoten zwecks Eröffnung einer Remotesteuerungssitzung überprüft der Core die Datenbank, um sicherzustellen, dass der die Anfrage initiierende Teilnehmer berechtigt ist, das Gerät anzuzeigen. Wird das Gerät nicht in der Datenbank geführt, lehnt der Core die Anforderung ab.

So kopieren Sie eine Gruppe mit Zertifikaten/privaten Schlüsseln von einem Coreserver auf einen anderen

1. Öffnen Sie auf dem Quell-Coreserver den Ordner \Programme\LANDesk\Shared Files\Keys.
2. Kopieren Sie die Dateien <Schlüsselname>.key, <Schlüsselname>.crt und <hash>.0 des Quellservers auf eine Diskette oder an einen anderen sicheren Speicherort.
3. Kopieren Sie auf dem Ziel-Coreserver die Dateien vom Quell-Coreserver in denselben Ordner (\Programme\LANDesk\Shared Files\Keys). Die Schlüssel werden umgehend angewendet.

Gehen Sie umsichtig vor, damit der private Schlüssel <Schlüsselname>.key nicht gefährdet wird. Der Coreserver verwendet diese Datei, um Geräte zu authentifizieren, und jeder Computer mit der Datei <Schlüsselname>.key kann Remoteausführungen und Dateiübertragungen an ein Management Suite-Gerät durchführen.

Bereitstellen von Agenten für nicht-persistente VDI-Abbilder

Wenn Sie Agenten für nicht-persistente Virtual-Desktop-Interface (VDI)-Abbilder zur Desktopvirtualisierung erstellen, sind einige zusätzliche Schritte erforderlich.

Der Agentenkonfigurationsprozess fügt für das betreffende Gerät Registrierungseinträge für die eindeutige Kennung und zur Verfolgung des Anmeldeverlaufs hinzu. In einer nicht-persistenten Umgebung gehen diese Daten beim Zurücksetzen des Abbilds verloren.

Wenn Sie sicherstellen wollen, dass Management Suite jeden Computer im VDI-Pool einzeln verfolgt, müssen Sie diese Registrierungseinträge aus dem Basisabbild löschen. Diese Vorgehensweise sorgt dafür, dass die Registrierungsschlüssel neu erstellt werden, wenn die einzelnen Computer im VDI-Pool das erste Mal gestartet und der Agent geladen wird.

Im Folgenden sind die Registrierungsschlüssel für die eindeutige Kennung (UniqueID) und die Verfolgung der Anmeldungen (Logons) aufgeführt, die Sie aus dem VDI-Basisabbild löschen müssen.

Bei 64-Bit-VDI-Abbildern:

```
HKLM\SOFTWARE\Wow6432Node\Intel\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\Wow6432Node\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\Wow6432Node\LANDesk\Inventory\LogonHistory\Logons
```

Bei 32-Bit-VDI-Abbildern:

```
HKLM\SOFTWARE\Intel\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\LANDesk\CommonApi\UniqueID
HKLM\SOFTWARE\LANDesk\Inventory\LogonHistory\Logons
```

Wenn Sie die Funktion für die Überwachung der Softwarenutzung verwenden, müssen Sie ferner einen UNC-Pfad für die Speicherung der Datendateien der Softwareüberwachung angeben. Wenn Sie keinen Pfad angeben, speichert die Softwarelizenzüberwachung die Überwachungsdaten in der Registrierung. In einer nicht-persistenten Umgebung gehen diese Daten beim Zurücksetzen des Abbilds verloren.

So zeichnen Sie statistische Daten zur Softwarenutzung an einer Netzwerkadresse auf

1. Klicken Sie auf **Extras > Agentenkonfiguration**.
2. Doppelklicken Sie auf die Agentenkonfiguration, die Sie in Ihrem VDI-Abbild verwenden werden.
3. Klicken Sie auf **Standard LANDesk Agent** > **Softwarenutzungsüberwachung**.
4. Wählen Sie **Softwareüberwachung verwenden** aus.
5. Wählen Sie **Statistische Daten zur Softwarenutzung an einer Netzwerkadresse aufzeichnen** aus.
6. Geben Sie die UNC-Pfadinformationen und die Anmeldeinformationen ein, die von den Agenten auf dem VDI-Abbild für den Zugriff auf diesen UNC-Pfad verwendet werden sollen.
7. Speichern Sie Ihre Änderungen.
8. Stellen Sie die Agentenkonfiguration für Ihr VDI-Basisabbild bereit.
9. Löschen Sie die zuvor in diesem Abschnitt erwähnten Registrierungsschlüssel für die eindeutige Kennung (UniqueID) und die Verfolgung der Anmeldungen (Logons).
10. Speichern Sie die Änderungen in Ihrem VDI-Basisabbild.

Deinstallieren von Geräteagenten

Vor Management Suite 8.5 war es jedem Benutzer möglich, Management Suite-Agenten durch Ausführen von wscfg32.exe mit dem Parameter /u zu deinstallieren. Da sich wscfg32.exe in der LDLogon-Freigabe befand, auf die verwaltete Geräte Zugriff hatten, war es relativ einfach, Management Suite-Agenten zu deinstallieren.

Seit Management Suite 8.5 gibt es den Parameter /u in der Datei wscfg32.exe nicht mehr. Es gibt jetzt ein neues Programm mit dem Namen "UninstallWinClient.exe" in der LDMain-Freigabe – dem wichtigsten Management Suite-Programmordner. Nur Administratoren haben Zugriff auf diese Freigabe. Dieses Programm deinstalliert Management Suite- oder Server Manager-Agenten auf allen Geräten, auf denen es ausgeführt wird. Sie können es in jeden gewünschten Ordner verschieben oder zu einem Anmeldeskript hinzufügen. Es handelt sich dabei um eine Windows-Anwendung, die im Hintergrund ausgeführt wird (ohne eine Benutzeroberfläche einzublenden).

Durch das Ausführen dieses Programms werden keine Geräte aus der Coredatenbank entfernt. Wenn Sie Agenten erneut auf einem Gerät bereitstellen, auf dem dieses Programm ausgeführt wurde, wird das betreffende Gerät in der Datenbank als neues Gerät gespeichert.

Konfigurieren von Linux- und UNIX-Geräteagenten

Sie können LANDesk Management Suite zur Verwaltung unterstützter Linux/UNIX-Distributionen verwenden. Informationen zu den unterstützten Linux/UNIX-Versionen und Anweisungen zu deren Installation finden Sie auf der LANDesk Linux\UNIX-Landingpage der LANDesk Benutzercommunity unter http://community.landesk.com/support/docs/DOC-10608.

Hilfe zu verwalteten Geräten

Im Fenster **Agentenkonfiguration** (**Extras > Konfiguration > Agentenkonfiguration**) können Sie die Konfigurationen für Geräteagenten bearbeiten. Mithilfe des Dialogfelds **Agentenkonfiguration** können Sie angeben, welche Agenten installiert werden und welche Optionen für diese Agenten gelten sollen. Sie können beliebig viele Agentenkonfigurationen erstellen. Es kann jedoch nur eine Standardkonfiguration geben. Sie können mit den Optionen in diesem Fenster Windows-, Macintosh-, Linux- und Server-Agentenkonfigurationen erstellen.

So erstellen Sie eine Konfiguration

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie auf die Schaltfläche **Neu**, um eine neue Windows-Konfiguration zu erstellen. Klicken Sie auf die Schaltfläche **Neuer Macintosh**, um eine neue Macintosh-Konfiguration zu erstellen.
3. Geben Sie, wie in den nachfolgenden Abschnitten beschrieben, Daten in das Dialogfeld **Agentenkonfiguration** ein. Klicken Sie auf **Hilfe** auf der jeweiligen Seite, um weitere Informationen zu erhalten.

HINWEIS: Wenn Sie das Dialogfeld **Agentenkonfiguration** zum Erstellen einer neuen Standardagentenkonfiguration verwenden, sollten Sie berücksichtigen, dass alle Geräte, die von WSCFG32 mithilfe von Anmeldeskripten konfiguriert werden, bei der nächsten Anmeldung automatisch mit den neuen Standardkonfigurationseinstellungen erneut konfiguriert werden, auch wenn ihre aktuellen Einstellungen mit den neuen Standardeinstellungen identisch sind.

In den nachstehenden Abschnitten werden die Seiten des Dialogfelds **Agentenkonfiguration** beschrieben.

Informationen zur Startseite

Die Startseite des Dialogfelds **Agentenkonfiguration** bietet die folgenden Optionen:

- **Konfigurationsname:** Diese Option wird über den Dialogfeldseiten eingeblendet. Geben Sie einen Namen ein, der die Konfiguration beschreibt, an der Sie zurzeit arbeiten. Dies kann ein bereits vorhandener oder ein neuer Konfigurationsname sein. Dieser Name wird im Fenster **Agentenkonfiguration** angezeigt.
- **Standardkonfiguration:** Bei Auswahl dieser Option wird diese Konfiguration als die Standardkonfiguration definiert, die installiert wird, wenn keine andere Konfiguration angegeben wird.

Die zu installierenden Agentenkomponenten (Standard):

- **Standard LANDesk Agent:** Installiert den Standard LANDesk Agenten, der als Basis für die Kommunikation zwischen Gerät und Coreserver dient. Diese Option ist eine erforderliche Option. Sie können sie zwar nicht deaktivieren, jedoch die mit ihr verknüpften Komponenten anpassen. (Beachten Sie, dass der Sicherheitsscanner automatisch mit dem Standard LANDesk Agenten installiert wird, Sie ihn jedoch mit den nachstehend auf der Seite "Sicherheit und Patch" aufgeführten Optionen konfigurieren.)
- **Benutzerdefinierte Datenformulare:** Blendet ein von den Benutzern auszufüllendes Formular ein. Sie können die von Benutzern eingegebenen Daten in der Coredatenbank abfragen. Verwenden Sie das Formular, um benutzerdefinierte Informationen direkt von Benutzern abzurufen.
- **Remotesteuerung:** Hiermit können Sie ein Gerät oder einen Server von einem beliebigen Netzwerkstandort aus steuern. Sorgt mit einem zentralen Helpdesk dafür, dass Kundenprobleme deutlich schneller gelöst werden. Verwenden Sie diese Option zur Remotesteuerung von Geräten im LAN/WAN.

Energieverwaltung:

- **Energieverwaltung:** Gibt Ihnen die Möglichkeit, den Energieverbrauch der von Ihnen verwalteten Geräte von einem zentralen Ort zu steuern. Sie können Richtlinien zur Energieverwaltung erstellen und bereitstellen und Berichte zur Bewertung der finanziellen Einsparungen und der Energieeinsparungen generieren. Ferner legen Sie die Bedingungen fest, unter denen Computer und Bildschirme in den Ruhezustand oder den Standby-Modus versetzt oder heruntergefahren werden. Benutzer können jedoch bestimmte Energieverwaltungsaktionen über eine clientseitige Benutzerschnittstelle verzögern, um sicherzustellen, dass nicht gespeicherte Daten nicht verloren gehen.

Verteilung:

- **Softwareverteilung:** Automatisiert die Installation von Softwareanwendungen oder die Verteilung von Dateien an Geräte. Verwenden Sie diese Option, um Anwendungen gleichzeitig auf mehreren Geräten zu installieren oder um Dateien oder Treiber auf mehreren Geräten zu aktualisieren.

Sicherheit:

- **LANDesk Antivirus:** Installiert den Antivirus-Agenten auf verwalteten Geräten. Antivirus sucht und identifiziert mithilfe des Sicherheitsscanners (der mit dem Standard LANDesk Agenten installiert wird) Viren auf verwalteten Geräten und stellt Optionen für die Handhabung infizierter Dateien und Ordner bereit. Administratoren laden Virendefinitionsupdates herunter und konfigurieren Virenscans auf der Konsole. So wird beispielsweise festgelegt, wie der Antivirus-Client auf verwalteten Geräten angezeigt wird und welche Optionen dem Endanwender zur Verfügung stehen. Sie müssen zuerst das Kontrollkästchen **Antivirus** auf der Seite **Start** der Agentenkonfiguration aktivieren, um die Seite **Antivirus** unter **Sicherheit** konfigurieren zu können.

- **Endpunktsicherheit:** Installiert den Agenten für Endpunktsicherheit auf verwalteten Geräten. Endpunktsicherheit schützt Ihre verwalteten Geräte vor Zero-Day-Angriffen, Firewallangriffen und dem Anschluss von nicht autorisierten Geräten. Die Endpunktsicherheitsdienste umfassen die folgenden drei Sicherheitskomponenten, die sich gegenseitig ergänzen: HIPS, LANDesk Firewall und Gerätesteuerung.

Echtzeitinventar und Überwachung:

Unterstützt mehrere Methoden zur Überwachung des Systemzustands eines Geräts. Während Alarmregelsätze auf der Coreserverkonsole definiert und auf mehreren Geräten bereitgestellt werden, können Sie auf einzelnen Geräten auch Leistungsüberwachungszähler zur Überwachung bestimmter Leistungspunkte definieren.

- **Baselinekomponenten:** Installiert einen Agenten, der die Systemhardware überwacht, wie etwa Lüftergeschwindigkeiten, Festplattenspeicher und die Gesamttemperatur des Geräts.
- **Erweiterte Komponenten:** Installiert einen Agenten, der Systemprozesse, Dienste und die Gesamtleistung überwacht.

Andere Optionen:

- **Alle auswählen:** Hiermit werden alle Agenten ausgewählt, die in der Liste **Zu installierende Agenten** aufgeführt sind.
- **Alle löschen:** Löscht alle verfügbaren Agenten in der Liste **Zu installierende Agenten** mit Ausnahme des obligatorischen Standard LANDesk Agenten.
- **Standardwerte:** Hiermit werden alle Agenten in der Liste **Zu installierende Agenten** ausgewählt, mit Ausnahme der Sicherheitsagenten.
- **Während der Installation einen vollständigen Inventarscan ausführen:** Führen Sie nach der Installation der Konfiguration auf den Clients einen vollständigen Inventarscan aus. Der Standard ist "aktiviert".
- **Startmenü auf Endbenutzergeräten anzeigen:** Wenn diese Option aktiviert ist, werden Windows-Startmenü-Einträge für installierte Agenten erstellt, die über eine Benutzeroberfläche verfügen. Wenn diese Option deaktiviert wird, werden die Agenten zwar installiert, aber es werden keine Einträge im Startmenü erstellt.
- **Temporäres Installationsverzeichnis:** Gibt den temporären Ordner an, der während der Installation eines Agenten auf verwalteten Geräten verwendet wird. Damit die Agenteninstallation ordnungsgemäß ausgeführt wird, darf dieser Ordner nicht schreibgeschützt sein.

Bereitstellen des Standard LANDesk Agenten

Für alle Management Suite Komponenten wird der Standard LANDesk Agent (vormals CBA) benötigt. Dieser Agent wird standardmäßig bei allen Geräteinstallationen installiert. Der Standard LANDesk Agent unterstützt u.a. die Geräteerkennung und verwaltet die Coreserver/Gerätekommunikation.

Der Standardagent umfasst standardmäßig den LANDesk Security Suite Sicherheitsscanner.

Verwenden Sie die Standard LANDesk Agent-Seiten, um die folgenden Komponenten und Einstellungen des Standard LANDesk Agent zu konfigurieren:

- Inventarscanner
- Local Scheduler
- Bandbreitenerkennung
- Neustartoptionen für das Gerät

Informationen zur Seite "Standard LANDesk Agent"

Verwenden Sie diese Seite, um die zertifikatbasierte Sicherheit zu konfigurieren und um festzulegen, welcher Bereich den Geräten, die mit dieser Konfiguration arbeiten, zur Verfügung gestellt wird.

Vertrauenswürdige Zertifikate

Wählen Sie die Coreserver-Zertifikate aus, die von den Geräten akzeptiert werden sollen. Geräte kommunizieren nur mit Cores und Konsolen, für die sie Zertifikate besitzen. Weitere Informationen zu den Zertifikaten und zum Kopieren von Zertifikaten von anderen Coreservern (um sie hier auswählen zu können) finden Sie unter "Agentensicherheit und vertrauenswürdige Zertifikate" auf Seite 114.

Unterhalb des Feldes für die vertrauenswürdigen Zertifikate können Sie den Coreserver ändern, mit dem Geräte kommunizieren, die diese Agentenkonfiguration verwenden. Dieses Feld enthält standardmäßig den aktuellen Coreserver. Der Name des Coreservers kann entweder der Name eines Windows-Computers, eine IP-Adresse oder ein vollständig qualifizierter Domänenname sein. Ein vollständig qualifizierter Domänenname für einen Core ist u. U. erforderlich, wenn Sie Agentenkonfigurationen mit einer Pushprozedur auf Geräten in unterschiedlichen Domänen bereitstellen, oder wenn ein Gerät den Namen des Coreservers nur auflösen kann, wenn dieser vollständig qualifiziert ist. Verwaltete Geräte verwenden die hier von Ihnen eingegebenen Informationen für die Kommunikation mit dem Coreserver. Stellen Sie deshalb sicher, dass der von Ihnen eingegebene Name von allen Geräten aufgelöst werden kann, die diese Konfiguration erhalten.

Der Name des Coreservers, den Sie hier als Teil einer Agentenkonfiguration eingeben, wird an folgender Position zur Registrierung des Geräts hinzugefügt:

- HKLM\Software\Intel\LANDesk\LDWM\CoreServer

Sobald Sie vertrauenswürdige Zertifikate ausgewählt und den Namen des Coreservers ggf. geändert haben, steht einem Kommunikationstest nichts mehr im Wege. Wenn Sie auf **Testen** klicken, wird ein Meldungsfeld eingeblendet, in dem mitgeteilt wird, ob der von Ihnen eingegebene Gerätename oder die von Ihnen eingegebene IP-Adresse aufgelöst werden konnte. Beachten Sie, dass die Schaltfläche **Testen** weder einen Ping-Test mit dem von Ihnen eingegebenen Gerät durchführt noch sicherstellt, dass der Name oder IP-Adresse zu einem Coreserver gehört.

Speicherort (Bereich)

Wenn Geräte in Bereiche eingeschlossen werden sollen, die auf benutzerdefinierten Verzeichnissen basieren, geben Sie einen Verzeichnispfad in das Feld **Pfad** ein. Der von Ihnen hier eingegebene Pfad definiert das Computerstandort-Inventarattribut des Geräts. Die Bereiche werden von der rollenbasierten Management Suite-Administration zum Steuern des Benutzerzugriffs auf Geräte verwendet und können auf diesem benutzerdefinierten Verzeichnispfad basieren.

Das Format der benutzerdefinierten Verzeichnispfade ähnelt dem eines Dateipfads, wobei die einzelnen Segmente jedoch durch Schrägstriche getrennt werden. Wenn Sie benutzerdefinierte, verzeichnisbasierte Bereiche verwenden möchten, müssen Sie zuerst entscheiden, in welche Kategorien Sie Ihre Geräte für die rollenbasierte Administration einteilen möchten. Sie können Geräte beispielsweise nach Gebiet, Abteilungs- oder Gruppenname oder einem anderen verwaltungstechnischen Detail Ihrer Wahl einteilen.

Verzeichnispfade, die Sie hier als Teil einer Agentenkonfiguration eingeben, werden an folgender Position zur Registrierung des Geräts hinzugefügt:

- HKLM\Software\Intel\LANDesk\Inventory\ComputerLocation

Sie müssen dieses Feld nicht ausfüllen. Wenn Sie dieses Feld leer lassen, wird das Computerstandort-Attribut des Geräts durch seinen Active Directory- oder eDirectory-Pfad definiert.

Wenn der Inventarscanner auf einem Gerät ausgeführt wird, zeichnet er das Computerstandort-Attribut des Geräts auf. Wenn Sie einen benutzerdefinierten Verzeichnispfad in das Feld **Pfad** eingegeben haben, ist dieser Pfad das Verzeichnis, das vom Scanner aufgezeichnet wird. Wenn Sie keinen benutzerdefinierten Verzeichnispfad eingegeben haben, versucht der Scanner, den Active Directory- oder NetWare eDirectory-Pfad des Geräts in das Computerstandort-Inventarattribut zu schreiben. Wenn weder ein benutzerdefinierter Verzeichnispfad noch ein LDAP-konformes Verzeichnis gefunden wird, wird das Computerstandort-Attribut nicht definiert. Dennoch lässt sich das Gerät nach wie vor in Abfrage- oder Gerätegruppenbereichen nachweisen.

Wenn Sie mehr darüber erfahren möchten, wie Bereiche in der rollenbasierten Administration von Management Suite eingesetzt werden und wie Sie einen Bereich mithilfe von benutzerdefinierten Verzeichnispfaden erstellen können, lesen Sie die Ausführungen unter "Benutzerverwaltung" auf Seite 40.

Informationen zur Seite "Inventarscanner" (unter "Standard LANDesk Agent")

Die Seite **Inventarscanner** des Dialogfelds **Agentenkonfiguration** bietet die folgende Funktionen:

- **Manuelles Update:** Die während der Softwarescans zum Ausschließen von Titeln verwendete Softwareliste wird in jedes Remotegerät geladen. Immer, wenn die Softwareliste von der Konsole aus geändert wird, müssen Sie sie manuell erneut an die Remotegeräte weiterleiten.
- **Automatisches Update:** Remotegeräte lesen die Softwareliste des Coreservers während des Softwarescans. Wenn diese Option ausgewählt ist, muss jedes Gerät über ein Laufwerk verfügen, das dem Verzeichnis ldlogon auf dem Coreserver zugewiesen wurde, damit es auf die Softwareliste zugreifen kann. In der Softwareliste erfolgte Änderungen stehen den Geräten sofort zur Verfügung.
    - **Aktualisierung mit HTTP:** Seit Management Suite 8 kann der Inventarscanner für LdAppl3.ini-Dateiübertragungen HTTP verwenden. Dadurch unterstützt der Scanner Targeted Multicast-Funktionen wie Polite-Bandbreite und Peerdownload. Mit einem Peerdownload können Geräte, die LdAppl3.ini-Updates benötigen, auf dem Coreserver nach dem Datum der neuesten Version suchen. Anschließend können die Geräte dann eine Verbindung zu Peers im Subnetz herstellen, um zu ermitteln, ob ein Peer das Update in seinem Multicast-Cache gespeichert hat. Verfügt ein Peer über das Update, erfolgt der Dateitransfer im lokalen Subnetz, ohne Netzwerkverkehr über Router oder WAN-Verbindungen zu erzeugen.

Inventarscans ausführen:

- **Ereignisbedingte Scans:** Konfiguriert den Zeitplan des Inventarscanners auf dem verwalteten Gerät. Standardmäßig ist der Scan so eingestellt, dass das Gerät einmal pro Tag gescannt und die Ergebnisse an den Coreserver zurückgemeldet werden.
- **Wenn sich der Benutzer anmeldet:** Führt den Inventarscanner aus, wenn sich der der Benutzer beim verwalteten Gerät anmeldet.
- **Max. zufällige Verzögerung:** Gibt einen Zeitrahmen vor, innerhalb dessen der Task ausgeführt werden kann. Diese Verzögerung sorgt dafür, dass Tasks, die bei der Anmeldung ausgeführt werden, nicht alle gleichzeitig ausgeführt werden (vorausgesetzt, dass das Verzögerungsintervall lang genug ist).
- **Wenn sich die IP-Adresse ändert (nur reduzierter Scan):** Der an die IP-Adresse gekoppelte Trigger sendet nur einen Miniscan an den Coreserver. Dies beschleunigt den Inventarscan bei IP-Adressänderungen.

- **Einstellungen ändern:** Hier können Sie die Einstellungen ändern und einen benutzerdefinierten Zeitplan konfigurieren, der auf Folgendem basiert: Uhrzeit, Wochentag, Monat, angemeldeter Benutzer, IP-Adressänderung und verfügbare Bandbreite. Der Standardzeitplan umfasst einen täglichen Scan mit einer zufälligen Verzögerung von maximal einer Stunde.

Informationen zur Seite "Local Scheduler" (unter "Standard LANDesk Agent")

Mit dem Local Scheduler Agent kann Management Suite Gerätetasks abhängig von der Tageszeit oder der verfügbaren Bandbreite starten. Der Local Scheduler Agent ist besonders für mobile Computer nützlich, die nur zeitweise mit dem Netzwerk verbunden sind oder sich über eine DFÜ-Verbindung in das Netzwerk einwählen. Sie können Local Scheduler beispielsweise so konfigurieren, dass eine Paketverteilung an mobile Computer nur zulässig ist, wenn diese Geräte mit dem WAN verbunden sind.

Beim Planen von Softwarepaketverteilungen oder Definieren von Anwendungsrichtlinien können Sie angeben, welche Bandbreite für die Verteilung der Pakete oder Richtlinien vorausgesetzt wird.

Der Local Scheduler wird auf Windows-Geräten als Dienst ausgeführt.

Die Seite **Local Scheduler** enthält die folgenden Funktionen:

- **Zeitabstand, in dem der Agent die lokale Registry nach Tasks abfragt:** Hiermit legen Sie fest, wie oft Local Scheduler nach Tasks sucht. Der Standardwert ist 10 Sekunden. Das von Ihnen ausgewählte Abfrageintervall wird auf dem lokalen Computer gespeichert.
- **Bandbreitenerkennung-Frequenz:** Wie oft Local Scheduler die Bandbreite überprüfen soll. Der Standardwert ist 120 Sekunden. Bandbreitenprüfungen finden nur statt, wenn ein geplanter Task vorliegt.

Informationen zur Seite "Alarmierung" (unter "Standard LANDesk Agent")

Alarmregelsätze definieren, welche Ereignisse sofortige Maßnahmen verlangen oder für Ihre Kenntnisnahme protokolliert werden sollen. Ein Regelsatz enthält diverse Alarmregeln, von denen jeder eine entsprechende Alarmaktion zugewiesen ist. Wenn Sie einen Alarmregelsatz definieren, können Sie ihn auf einem oder mehreren Geräten bereitstellen, um die Elemente zu überwachen, die für diese Art von Gerät wichtig sind.

Sie können einen der vordefinierten Regelsätze oder Regelsätze, die Sie selbst innerhalb des Alarm-Tools erstellt haben, bereitstellen.

Die Alarmseite enthält die folgenden Funktionen:

- **Hinzufügen:** Klicken Sie auf **Hinzufügen**, um der Liste **Ausgewählter Alarmregelsatz** einen bestehenden Regelsatz hinzuzufügen. Die Regelsätze in dieser Liste werden auf Geräten bereitgestellt, die diese Agentenkonfiguration erhalten.
- **Entfernen:** Klicken Sie auf einen Regelsatz und dann auf **Entfernen**, um ihn aus der Liste **Ausgewählter Alarmregelsatz** zu entfernen.

Informationen zur Seite "Bandbreitenerkennung" (unter "Standard LANDesk Agent")

Mit der Funktion "Bandbreitenerkennung" lässt sich die Bandbreite zwischen Geräten und Coreserver ermitteln. Sie können Management Suite Aktionen (beispielsweise die Verteilung von Softwareprodukten) von der verfügbaren Bandbreite abhängig machen. Verwenden Sie diese Option, wenn Remotegeräte oder Geräte, die über eine langsame Verbindung auf das Netzwerk zugreifen, vorhanden sind.

Die Seite **Bandbreitenerkennung** des Dialogfelds **Agentenkonfiguration** umfasst die folgende Funktionen:

- **Bandbreitenerkennungsmethode wählen:** Geben Sie an, ob ICMP oder PDS für die Bandbreitenerkennung verwendet werden soll. ICMP sendet ICMP-Echoanforderungen verschiedener Größe an die Remotegeräte und bestimmt anhand der Antwortzeit dieser Echoanforderungen/-reaktionen die ungefähre Bandbreite. ICMP unterscheidet auch zwischen LAN (Hochgeschwindigkeit) und WAN (langsame Verbindung, jedoch kein DFÜ). Nicht alle Router oder Geräte unterstützen jedoch ICMP-Echoanforderungen.
  Wenn Ihre Netzwerkkonfiguration keine ICMP-Echoanforderungen zulässt, können Sie PDS wählen. Die PDS-Bandbreitentests sind zwar nicht so detailliert wie ICMP, finden jedoch entweder eine LAN- oder RAS-Verbindung (in der Regel DFÜ-Verbindung) mit geringer Bandbreite. Die PDS-Methode funktioniert nur, wenn der PDS-Dienst auf dem Server ausgeführt wird. Sie können diesen Dienst installieren, indem Sie den Standard LANDesk-Agent auf dem Paketserver bereitstellen.
- **LAN-Grenzwert in Bit pro Sekunde:** Der Grenzwert, der eine Verbindung als WAN und nicht als LAN klassifiziert. Der Standardwert ist 262.144 Bit/s.

Informationen zur Seite "Neustartoptionen für das Gerät" des Dialogfelds "Agentenkonfiguration" (unter "Standard LANDesk Agent")

Sobald Sie auf den Geräten Management Suite Agenten installiert haben, muss möglicherweise ein Neustart durchgeführt werden, um die Agentenkonfiguration abzuschließen. Die Seite **Neustartoptionen für das Gerät** des Dialogfelds **Agentenkonfiguration** umfasst die folgenden Funktionen:

- **Geräte nach Konfiguration nicht neu starten:** Die Geräte werden nicht neu gestartet, auch wenn die ausgewählten Komponenten einen Neustart erforderlich machen. Sollte ein Neustart erforderlich sein, funktionieren die Komponenten erst ordnungsgemäß, nachdem das Gerät neu gestartet wurde.
- **Geräte bei Bedarf neu starten:** Die Geräte werden nur neu gestartet, wenn eine bestimmte Komponente einen Neustart erforderlich macht.
- **Neu starten mit Benutzeroption zum Abbruch:** Falls ein bestimmter Agent einen Neustart erforderlich macht, können die Benutzer den Neustart abbrechen. Sollte ein Neustart erforderlich sein, funktionieren die Komponenten erst ordnungsgemäß, nachdem das Gerät neu gestartet wurde. Sie können einen Timeoutwert auswählen, mit dem festgelegt wird, wie lange die Neustartaufforderung auf dem Bildschirm des Benutzers angezeigt wird, ehe der Computer neu gestartet wird. Dieser Timeoutwert ist für Benutzer sinnvoll, die während der Bereitstellung nicht an ihrem Computer sitzen.
- **Benutzer darf den Neustart innerhalb dieses Zeitraums abbrechen:** Wenn Sie Benutzern die Möglichkeit zur Stornierung des Neustarts geben möchten, bevor dieser automatisch ausgeführt wird, geben Sie ein, wie lange die Neustartmeldung angezeigt werden soll.

Informationen zur Seite "Überwachung der Softwarenutzung" (unter "Standard LANDesk Agent")

Die Seite **Überwachung der Softwarenutzung** wird dazu verwendet, die Nutzungsstatistik für die Softwarelizenzüberwachung zu verfolgen. Diese Funktion sammelt Informationen zur drei verschiedenen Datentypen: Nutzungsstatistik aus der Softwarelizenzüberwachung, zusätzliche Inventarinformationen und Merkmale für die Blockierung von Anwendungen.

Wenn Sie Agenten für nicht-persistente Virtual Desktop Interface (VDI)-Datenträgerabbilder bereitstellen, müssen Sie einen UNC-Pfad festlegen, in dem die Datendateien der Softwareüberwachung gespeichert werden, Wenn Sie keinen Pfad angeben, speichert die Softwarelizenzüberwachung die Überwachungsdaten in der Registrierung. In einer nicht-persistenten Umgebung gehen diese Daten beim Zurücksetzen des Abbilds verloren. Weitere Informationen finden Sie unter "Bereitstellen von Agenten für nicht-persistente VDI-Abbilder" auf Seite 117.

Das Fenster **Überwachung der Softwarenutzung** enthält die folgenden Optionen:

- **Softwareüberwachung verwenden:** Ermöglicht die Verfolgung von Software durch Softwarelizenzüberwachung, Inventarscans und die Blockierung von Anwendungen durch die Funktion "Anwendungsblocker".
- **Statistische Daten zur Softwarenutzung an einer Netzwerkadresse aufzeichnen** Wählen Sie diese Option und konfigurieren Sie die zugehörigen Einstellungen, wenn Sie diese Agentenkonfiguration für ein nicht-persistentes VDI-Abbild bereitstellen.
- **UNC-Pfad, in dem die Datendateien der Softwareüberwachung gespeichert werden:** Der UNC-Pfad, den Sie verwenden wollen, mit folgendem Format: \\Servername\Freigabename.
- **Domäne\Benutzername:** Die Benutzeranmeldeinformationen, die Zugriff auf den UNC-Pfad ermöglichen.
- **Kennwort** und **Kennwort bestätigen**: Das Kennwort für das von Ihnen angegebene Benutzerkonto.

Bereitstellen benutzerdefinierter Datenformulare

Sie können benutzerdefinierte Datenformulare erstellen und verteilen, um Gerätedaten zu erheben, die die in der Coredatenbank verfügbaren Standardinformationen ergänzen. Die Formulare, die Sie mit dem Formular-Designer anlegen, können mit einem Gerätebereitstellungsdienst oder mit dem Dialogfeld **Agentenkonfiguration** verteilt werden.

Verwenden Sie den Formular-Designer, um Formulare, die Sie an die Geräte in Ihrer Verwaltungsdomäne verteilen, Ihren Anforderungen entsprechend anzupassen. Weitere Informationen finden Sie unter "Verwenden von benutzerdefinierten Datenformularen" auf Seite 163.

Informationen zur Seite "Benutzerdefinierte Datenformulare"

Der Abschnitt für die benutzerdefinierten Datenformulare besteht aus zwei Seiten. Die Seite **Benutzerdefinierte Datenformulare** bietet folgende Funktionen:

- **Manuelle Formularaktualisierung:** An jedes Gerät werden ausgewählte Formulare verteilt. Wenn sich die Formulare ändern oder neue Formulare hinzukommen, müssen Sie die Formulare manuell an die Remotegeräte neu verteilen.
- **Automatisches Update:** Remotegeräte durchsuchen den Coreserver bei jeder Ausführung des Inventarscanners (beispielsweise beim Start) auf aktualisierte Formulare. Für den Zugriff auf die aktualisierten Formulare muss auf jedem Gerät ein Laufwerk dem Verzeichnis ldlogon auf dem Coreserver zugewiesen sein.
- **Formulare Endanwendern anzeigen:** Wählen Sie aus, wie Remotegeräte auf benutzerdefinierte Formulare zugreifen:
    - **Beim Start:** Die ausgewählten Formulare werden automatisch beim Start auf allen Geräten ausgeführt.
    - **Während der Inventarscanner ausgeführt wird:** Die ausgewählten Formulare werden nur ausgeführt, wenn der Inventarscanner auf dem jeweiligen Gerät ausgeführt wird. Der Inventarscanner wird automatisch beim Start ausgeführt und Geräte können ihn jederzeit manuell ausführen.
    - **Beim Starten aus dem LANDesk Programmordner:** Die ausgewählten Formulare werden als Elemente im LANDesk-Ordner des Geräts angezeigt. Sie werden nicht automatisch ausgeführt.

Informationen zur Seite "Mit dem Agenten gesendete Formulare" des Dialogfelds "Agentenkonfiguration"

Auf der Seite **Mit dem Agenten gesendete Formulare** sind alle definierten Datenformulare aufgeführt. Wählen Sie, welche Formulare den Geräten, die diesen Konfigurationstask erhalten, zur Verfügung gestellt werden sollen. Damit Formulare in dieser Liste angezeigt werden, müssen Sie sie zuvor erstellen (**Extras > Konfiguration > Benutzerdefinierte Datenformulare**).

Bereitstellen der Softwareverteilung

Die Softwareverteilung automatisiert die Installation von Softwareanwendungen und die Verteilung von Dateien an Geräte. Verwenden Sie den Softwareverteilungsagenten, um auf mehreren Geräten gleichzeitig Anwendungen zu installieren oder Dateien oder Treiber zu aktualisieren.

Die Softwareverteilung benutzt einen Web- oder Dateiserver zum Speichern von Paketen. Die Geräte greifen beim Download eines Pakets auf diesen Paketserver zu. Sie müssen wie im Kapitel "Softwareverteilung" beschrieben einen Paketserver konfigurieren. Sie können den Softwareverteilungsagenten auf Geräten bereitstellen, bevor Sie einen Paketserver einrichten. Weitere Informationen finden Sie unter "Softwareverteilung/Verteilungspakete/Verteilungsmethoden" auf Seite 269.

Informationen zur Seite "Softwareverteilung"

Die Seite **Softwareverteilung** des Dialogfelds **Agentenkonfiguration** enthält die folgende Funktionen:

- **Client-Zielspeicherort:** Der Speicherort, an dem bereitgestellte, virtualisierte Anwendungen auf verwalteten Geräten gespeichert werden. Diese Option hat keinen Effekt, wenn Sie keine virtualisierten Anwendungen verteilen, die mit dem LANDesk Application Virtualization Add-on erstellt wurden.
- **LDAP-Zielgruppenadressierung aktivieren:** Gibt virtuellen Zugriff auf virtuelle Anwendungen, die bestimmten Organisationseinheiten (OUs) oder Gruppen aus einem Active Directory zugewiesen werden sollen.

Informationen zur Seite "Richtlinienoptionen" (unter "Softwareverteilung")

Mit dem richtlinienbasierten Verteilungsagenten können Sie mehrere Anwendungen gleichzeitig in Gerätegruppen installieren. Verwenden Sie diesen Agenten, um Gerätegruppen zu verwalten, die die gleiche Software benötigen.

Das LANDesk-Softwarebereitstellungsportal wird auf verwalteten Geräten ausgeführt und zeigt die verfügbare Software für dieses verwaltete Gerät. Um die verfügbare Software anzuzeigen, muss das Softwarebereitstellungsportal die Richtlinieninformationen regelmäßig vom Coreserver empfangen. Richtlinienupdates werden vorgenommen, wenn:

- ein Benutzer das LANDesk-Softwarebereitstellungsportal vom Windows Startmenü aus startet,
- bei der Anmeldung, wenn die Option **LANDesk Softwarebereitstellungsportal** bei Anmeldung ausführen ausgewählt ist.
- bei der Anmeldung, wenn die Option **Aktualisierung der Richtlinieninformationen vom Core bei Anmeldung ausführen** ausgewählt ist,
- im Local-Scheduler-Intervall, das Sie angeben, wenn Sie auf die Schaltfläche **Einstellungen ändern** klicken. In der Grundeinstellung verwenden verwaltete Geräte den Local-Scheduler, um einmal täglich Richtlinienupdates abzurufen.

Die Seite **Richtlinienoptionen** enthält die folgenden Funktionen:

- **Wenn Benutzer sich anmeldet:** Ist dieses aktiviert, dann aktualisiert das verwaltete Gerät die Richtlinieninformationen, nachdem sich ein Benutzer anmeldet. **Max. zufällige Verzögerung:** gibt dem Benutzer die Möglichkeit, das Update um die angegebene Zeit (in Stunden) zu verzögern.
- **Wenn sich die IP-Adresse ändert:** Wird diese Option ausgewählt, dann aktualisiert das verwaltete Gerät die Richtlinieninformationen, wenn sich die IP-Adresse ändert.
- **Einstellungen ändern:** Hier ändern Sie die Angabe, wie oft und wann der Local-Scheduler Richtlinienupdates abruft. Dieser Plan wird zusätzlich zu allen von Ihnen ausgewählten Anmeldeoptionen ausgeführt.

Informationen zur Seite "LaunchPad" (unter "Softwareverteilung")

Diese Seite verwenden Sie, um festzulegen, welche LaunchPad-Anpassungen Endbenutzer vornehmen dürfen. LaunchPad dient der Organisation von Links zu bereitgestellter Software auf verwalteten Geräten. Bei der bereitgestellte Software kann es sich um lokalem gehostete oder "Just in Time" installierte Anwendungen handeln. Die Seite "LaunchPad" enthält die folgenden Funktionen:

- **Benutzer können die Größe der LaunchPad-Fenster anpassen:** Gibt Benutzern die Möglichkeit, die Bereichsgröße anzupassen.
- **Benutzer können LaunchPad-Fenster verschieben und andocken:** Gibt Benutzern die Möglichkeit, Fenster an eine beliebige Stelle auf dem Desktop zu verschieben und anzudocken.

Informationen zur Seite "Portal" (unter "Softwareverteilung")

Auf der Seite "Portal" sind alle Softwareverteilungspakettasks aufgeführt, die unter Verwendung einer richtlinienbasierten Verteilungsmethode verteilt wurden. Diese Seite verwenden Sie, um die Darstellung des Portalfensters anzupassen.

Eine richtlinienbasierte Verteilungsmethode verhält sich insofern anders als ein Push, als die Anforderung der Richtlinien vom verwalteten Gerät initiiert werden muss. Dies bedeutet, dass das Paket nicht vom Coreserver auf das Gerät gepusht wird, sondern dass die zugehörigen Details in der Datenbank auf dem Coreserver gespeichert bleiben, bis das verwaltete Gerät eine Abfrage bezüglich zugewiesener richtlinienbasierter Softwareverteilungstasks an den Coreserver richtet. Beim Öffnen des Portals wird automatisch das Extra zur Richtliniensynchronisierung gestartet und die Liste wird mit den neuen, dem verwalteten Gerät zugewiesenen Tasks aktualisiert.

Die Seite **Portal** enthält die Felder **Optionale Spalten** und **Spalten und Reihenfolge anzeigen für Anwendung**. Diese Felder werden dazu verwendet, das Layout der Optionen zu ändern, die für die Anpassung zusätzlicher Informationen zu allen Paketen im Fenster "Softwarebereitstellungsportal" von LANDesk Desktop Manager auf dem verwalteten Gerät eingesetzt werden. Das Fenster **Softwarebereitstellungsportal** umfasst die Registerkarten **Verfügbar** und **Verlauf**, die in der Agentenkonfiguration auf der Seite **Portal** eingerichtet werden. Mithilfe des Felds **Optionale Spalten** können Sie die Spalten **Anwendung** und **Verlauf**, die auf den Registerkarten erscheinen, Ihren Anforderungen entsprechend anordnen und die Informationen in logischer Weise gruppieren.

Die Portalseite enthält die folgenden Funktionen:

- **Anwendung:** Zeigt Pakete an, die derzeit für eine vom Benutzer initiierte, optionale oder empfohlene Softwarebereitstellung verfügbar sind.
- **Verlauf:** Zeigt alle Pakete an, für die unter Verwendung des Portals über eine Richtlinie bereits eine Installation erfolgt ist oder versucht wurde.

- **Optionale Spalten:** Die Spalten, die im Fenster "Softwarebereitstellungsportal" von LANDesk Desktop Manager auf den Registerkarten **Anwendung** und **Verlauf** erscheinen.
  - **Größe:** Zeigt die physikalische Größe des Pakets an, damit der Benutzer Bescheid weiß, bevor er mit dem Download einer großen Anwendung fortfährt.
  - **Gruppe:** Gibt LANDesk Administratoren die Möglichkeit, bei jedem einzelnen Verteilungspakettask eine Gruppe für Anwendungen anzugeben, nach der der Endbenutzer die Liste der Anwendungen sortieren kann, wie beispielsweise nach Anwendungstyp, Anbieter oder Kategorie. Bei jedem einzelnen geplanten Task zur Softwareverteilung erfolgt eine Gruppenzuordnung.
  - **Beschreibung:** Zeigt die Beschreibung aus den Eigenschaften des Verteilungspakets an.
  - **Status:** Gibt an, ob die Installation erfolgreich ausgeführt wurde oder fehlgeschlagen ist.
  - **Letzte Ausführung:** Gibt das Datum und die Uhrzeit des letzten Versuchs einer Installation dieses Pakets an.
  - **Typ:** Gibt an, ob das Paket erforderlich, empfohlen oder optional ist.
- **Spalten und Reihenfolge anzeigen für Anwendung/Verlauf:** Zeigt die Standardspalten an, die im Fenster "Softwarebereitstellungsportal" von LANDesk Desktop Manager auf den Registerkarten "Anwendung" und "Verlauf" erscheinen. Die Standardliste umfasst Folgendes:
  - **Agent (erforderlich):** Zeigt den Namen des Verteilungspakets an.
  - **Beschreibung** (optional)
  - **Status** (optional)
  - **Letzte Ausführung** (optional)
  - **Typ** (optional)
  - Die Schaltflächen **Nach oben** und **Nach unten** verwenden Sie, um die Abfolge der Spalten anzupassen.

Bereitstellen der Remotesteuerung

Bei der Remotesteuerungsbereitstellung müssen Sie sich für ein Sicherheitsmodell entscheiden. Folgende Möglichkeiten stehen zur Auswahl:

- **Lokale Vorlage:** Als das einfachste Sicherheitsmodell verwendet die lokale Vorlage jede beliebige Remotesteuerungseinstellung, die auf dem Gerät angegeben ist. Dieses Modell verlangt keine zusätzliche Authentifizierung oder Gruppenmitgliedschaft.
- **Windows NT-Sicherheit/lokale Vorlage:** Dieses Sicherheitsmodell verwendet eine Windows NT-Remotesteuerungsoperatoren-Gruppe. Die Mitglieder dieser Gruppe sind berechtigt, Geräte remote zu steuern. Berechtigte Benutzer verwenden trotzdem die Remotesteuerungseinstellungen des Geräts, wie zum Beispiel "Berechtigung erforderlich".
- **Integrierte Sicherheit:** Dies ist der Standardwert und die sicherste Option. Die integrierte Sicherheit wird im nächsten Abschnitt beschrieben.

Informationen zur integrierten Sicherheit

Die integrierte Sicherheit ist das neue Standard-Sicherheitsmodell. Der Kommunikationsfluss der integrierten Remotesteuerungssicherheit sieht wie folgt aus:

1. Der Remote Control Viewer stellt eine Verbindung mit Remotesteuerungsagenten des verwalteten Geräts her. Daraufhin antwortet der Agent, dass die integrierte Sicherheitsauthentifizierung erforderlich

ist.

2. Der Viewer fordert Remotesteuerungsrechte vom Coreserver an.
3. Der Coreserver ermittelt die angeforderten Remotesteuerungsrechte basierend auf dem Bereich des Viewers, der rollenbasierten Administrationsrechte und der Active Directory-Rechte. Anschließend erstellt der Coreserver ein sicher signiertes Dokument und sendet es zurück an den Viewer.
4. Der Viewer sendet dieses Dokument an den Remotesteuerungsagenten auf dem verwalteten Gerät. Dort wird die Prüfung des signierten Dokuments vorgenommen. Wenn alles seine Ordnung hat, lässt der Agent den Remotesteuerungsvorgang zu.

WARNUNG: Die integrierte Sicherheit funktioniert nur mit Coreserver
Wenn der Coreserver bei Verwendung der integrierten Remotesteuerungssicherheit nicht verfügbar ist, sind die Konsolen nicht in der Lage, Geräte per Remotesteuerung zu bedienen. Die integrierte Sicherheit setzt den funktionsfähigen Coreserver voraus.

Verwenden der Windows NT-Sicherheit/lokale Vorlage mit Windows XP-Geräten

Damit die Windows NT-Sicherheit/Authentifizierung über lokale Vorlage bei Windows XP-Geräten funktioniert, müssen Sie die Geräte so konfigurieren, dass das Standard-Windows XP-Freigabe- und Sicherheitsmodell für lokale Konten verwendet wird (lokale Benutzer authentifizieren sich als sie selbst). Wenn Sie dies nicht tun, arbeitet die Gast-Standardauthentifizierung nicht mit der Windows NT-Sicherheit der Remotesteuerung zusammen.

So legen Sie das Standard-Windows XP-Sicherheitsmodell fest

1. Klicken Sie auf dem Windows XP-Gerät auf **Start > Systemsteuerung**.
2. Klicken Sie im Applet **Lokale Sicherheitsrichtlinie** unter **Verwaltung** auf **Sicherheitsoptionen > Netzwerkzugriff**: **Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten** und wählen Sie die Einstellung **Klassisch - lokale Benutzer authentifizieren sich als sie selbst**.

Informationen zur Seite "Remotesteuerung"

Die Seite **Remotesteuerung** verwenden Sie zur Auswahl und Konfiguration von Profilen für die Remotesteuerungseinstellungen. In diesem Dialogfeld können Sie auch die Treibereinstellungen ändern.

- **Wählen Sie die Remotesteuerungseinstellungen aus, die angewendet werden sollen:** Zeigt eine Liste der verfügbaren Profile für die Remotesteuerungseinstellungen. Sie können das Profil auswählen, das von dieser Agentenkonfiguration verwendet werden soll.
- **Konfigurieren:** Öffnet das Dialogfeld **Remotesteuerungseinstellungen konfigurieren**, in dem Sie die Profile für Remotesteuerungseinstellungen konfigurieren und verwalten können.
- **Spiegeltreiber verwenden:** Diese standardmäßig ausgewählte Option verwendet zur Verbesserung der Remotesteuerungsleistung auf Geräten den Remotesteuerungsspiegeltreiber.

- **Leerer Bildschirmtreiber verwenden:** Diese standardmäßig ausgewählte Option verwendet einen Spezialtreiber, der den Bildschirmtreiber des Zielgeräts anweisen kann, den Bildschirm zu deaktivieren. Wenn dieser Treiber aktiviert ist, filtert er Befehle, die an den echten Bildschirmtreiber gesendet werden, um zu verhindern, dass der Bildschirm wieder aktiviert wird. Remotesteuerungsoperatoren können das Deaktivieren des Bildschirms von der Remotesteuerungs-Viewer-Anwendung ein- oder ausschalten. Wenn bei Verwendung dieses Treibers Kompatibilitätsprobleme auftreten, deaktivieren Sie das Kontrollkästchen, um eine kompatiblere u. U. jedoch weniger effektive Methode der Bildschirmaktivierung zu verwenden. Wenn Sie die Treiber für die Bildschirmdeaktivierung nicht verwenden, kann die alternative Methode der Bildschirmdeaktivierung während der Remotesteuerungssitzung evtl. bewirken, dass der Bildschirm flackert. Für diese Option ist der Spiegeltreiber erforderlich.

Informationen zum Dialogfeld "Remotesteuerungseinstellungen konfigurieren"

Öffnet das Dialogfeld **Remotesteuerungseinstellungen konfigurieren**, in dem Sie Ihre Profile für Remotesteuerungseinstellungen verwalten können. Sie können mehrere Profile für Remotesteuerungseinstellungen erstellen und dasjenige auswählen, das als Standardprofil für neue Agentenkonfigurationen dienen soll.

- **Neu:** Erstellt ein neues Profile für Remotesteuerungseinstellungen.
- **Bearbeiten:** Bearbeitet ein vorhandenes Profil.
- **Kopieren:** Öffnet das ausgewählte Profil und fügt "Kopie von" an den Anfang des **Namens** des ausgewählten Profils ein. Wenn Sie auf **Speichern** klicken, wird es als ein neues Profil gespeichert.
- **Löschen:** Löscht das ausgewählte Profil. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
- **Ausgewählte verwenden:** Schließt das Dialogfeld **Remotesteuerungseinstellungen konfigurieren** und wählt das von Ihnen ausgewählte Profil als Einstellung im Dropdownlistenfeld **Wählen Sie die Remotesteuerungseinstellungen aus, die angewendet werden sollen** aus.

Informationen zur Seite "Allgemeine Einstellungen"

Die Seite **Remotesteuerung** des Dialogfelds **Agentenkonfiguration** enthält die folgende Funktionen:

- **Lokale Vorlage:** Verwendet nur die einfachen Berechtigungen des lokalen Geräts auf der Seite **Berechtigungen**.
- **Windows NT-Sicherheit/lokale Vorlage:** Nur Mitglieder der Gruppe "Remotesteuerungsoperatoren" dürfen Remotesteuerungsverbindungen zwischen Konsole und Remotegeräten initiieren. Genehmigte Benutzer müssen trotzdem den Berechtigungssatz der Seite "Remotesteuerungseinstellungen" in diesem Dialogfeld verwenden.
  Da es sich bei der Gruppe "Remotesteuerungsoperatoren" um eine lokale Gruppe handelt, besitzt jedes Gerät eine eigene Kopie der Gruppe. Um nicht jede Remotesteuerungsoperatoren-Gruppe eines jeden Geräts einzeln verwalten zu müssen, fügen Sie zu jeder lokalen Gruppe eine globale Gruppe (auf Domänenebene) hinzu.
  Berechtigte Benutzer verwenden trotzdem die Remotesteuerungseinstellungen des Geräts, wie zum Beispiel "Berechtigung erforderlich".
- **Integrierte Sicherheit:** Dies ist das weiter oben in diesem Abschnitt beschriebene Standard-Sicherheitsmodell. Berechtigte Benutzer müssen dennoch den Berechtigungssatz der Seite **Berechtigungen** verwenden.
- **HTML-Zugriff zulassen:** Lässt es zu, dass der Remotesteuerungsagent HTML-Remotesteuerungsanforderungen empfängt. Weitere Informationen finden Sie unter HTML-Remotesteuerung.

- **Als Standard festlegen:** Macht das Profil für Remotesteuerungseinstellungen, das Sie konfigurieren, zum Standardprofil für Remotesteuerungseinstellungen für neue Agentenkonfigurationen.

Hinzufügen von Benutzern zur Remotesteuerungsoperatoren-Gruppe und zur "Nur anzeigen"-Gruppe

Wenn Sie das Sicherheitsmodell **Windows NT-Sicherheit/Lokale Vorlage** ausgewählt haben, werden in den Feldern **Remotesteuerungsoperatoren-Gruppe** und **Gruppe "Nur anzeigen"** die Benutzer für die Konsole oder für die ausgewählte Windows NT-Domäne aufgeführt. Die hier ausgewählten Benutzer haben Remotesteuerungszugriff auf die Geräte, auf die die Einstellungen angewendet werden, die Sie in der Datei mit den Konfigurationseinstellungen festgelegt haben. Benutzer in der **Gruppe "Nur anzeigen"** können Remotegeräte nur anzeigen. Sie können weder die Bedienung der Maus noch der Tastatur übernehmen.

Beim Hinzufügen von Benutzern zu einer der Remotesteuerungsgruppen verwendet die Konsole zum Anzeigen der Benutzer in einer Domäne die Windows-Anmeldeinformationen des angemeldeten Benutzers, nicht die Anmeldeinformationen des Benutzers der LANDesk-Konsole. Wenn im Feld **Benutzer auflisten aus** nicht die gewünschte Domäne angezeigt wird, melden Sie sich bei Windows als ein Benutzer mit Rechten für diese Domäne an.

So treffen Sie Ihre Auswahl aus einem vorhandenen Server oder einer Domäne

1. Klicken Sie auf der Seite **Remotesteuerung** auf **Windows NT-Sicherheit/lokale Vorlage** und dann auf die Schaltfläche **Hinzufügen**.
2. Wählen Sie im Feld **Benutzer auflisten aus** entweder den Coreserver-Namen oder eine Windows NT-Domäne aus, die Benutzerkonten enthält.
3. Wählen Sie in der Benutzerliste einen oder mehrere Benutzer aus und klicken Sie auf **Einfügen**, um sie zur Liste **Eingefügte Namen** hinzuzufügen.
4. Klicken Sie auf **OK**, um die ausgewählten Namen zur Gruppe "Remotesteuerungsoperatoren" auf jedem Gerät hinzuzufügen, dem diese Konfigurationseinstellungen zugewiesen werden.
5. Wenn Sie einen dieser Benutzer in die **Gruppe "Nur anzeigen"** einfügen möchten, wählen Sie ihn aus und verschieben Sie ihn in die Gruppe. Benutzer können nur einer Gruppe angehören.

So geben Sie Namen manuell ein

Sie können Namen manuell eingeben, indem Sie in die Liste **Eingefügte Namen** klicken und Namen in einem der folgenden Formate eingeben. Zur Trennung von Namen verwenden Sie Strichpunkte.

- **DOMAIN\username**, wobei DOMAIN für den Namen jeder beliebigen Domäne steht, auf die das Zielgerät zugreifen kann.
- **MACHINE\username**, wobei MACHINE der Name eines Geräts ist, das sich in derselben Domäne wie das Zielgerät befindet.
- **DOMAIN\groupname**, wobei DOMAIN der Name einer Domäne ist, auf die das Zielgerät zugreifen kann, und "groupname" dem Namen einer Verwaltungsgruppe in dieser Domäne entspricht.
- **MACHINE\groupname** wobei MACHINE der Name eines beliebigen Geräts ist, das sich in derselben Domäne wie der verwaltete Knoten befindet, und "groupname" dem Namen einer Verwaltungsgruppe auf diesem Gerät entspricht.

Wenn Sie keinen Domänen- oder Gerätenamen angeben, wird angenommen, dass der angegebene Benutzer oder die Gruppe zum lokalen Gerät gehört.

Klicken Sie auf **OK**, um die Namen der Gruppe "Remotesteuerungsoperatoren" auf dem Zielgerät hinzuzufügen.

Informationen zur Seite "Indikatoren" (unter "Remotesteuerung")

Die Seite **Indikatoren** des Abschnitts **Remotesteuerung** umfasst die folgenden Funktionen:

- **Unverankertes Desktopsymbol:** Zeigt das Symbol für den Remotesteuerungsagenten entweder ständig oder nur dann auf dem Gerätebildschirm an, wenn das Gerät remote gesteuert wird. Bei der Steuerung durch die Konsole ändert sich das Symbol in eine Lupe und die Titelleiste des Symbols wird rot unterlegt.
- **Taskleistensymbol:** Fügt das Symbol für den Remotesteuerungsagenten in die Taskleiste ein. Auch bei dieser Funktion kann das Symbol ständig angezeigt werden oder nur, wenn das Gerät remote gesteuert wird.
- **Remotecomputer sperren, wenn die Sitzung beendet wird:** Sperrt das verwaltete Gerät im sicheren Modus, unabhängig davon, ob der Benutzer angemeldet ist oder nicht.

Informationen zur Seite "Berechtigungen" (unter "Remotesteuerung")

Die Seite **Berechtigungen** des Abschnitts **Remotesteuerung** enthält die folgenden Funktionen:

- **Remotesteuerung:** Erteilt die Berechtigung, das Gerät zu steuern.
- **Zeichnen:** Erteilt die Berechtigung zur Verwendung der Zeichenwerkzeuge im Viewer-Fenster des Geräts.
- **Nur anzeigen:** Remotesteuerungsoperatoren können das Gerät nur anzeigen, jedoch nicht remote mit ihm interagieren.
- **Chat:** Erteilt die Berechtigung zur Eröffnung einer Chat-Sitzung mit dem Gerät.
- **Dateiübertragung:** Erteilt die Berechtigung, Dateien auf die lokalen Laufwerke und von den lokalen Laufwerken des Geräts zu übertragen.
- **Anwendungen auf Remotegerät ausführen:** Erteilt die Berechtigung zur Ausführung von Programmen auf dem Gerät.
- Als Administrator ausführen: Führt das Programm unter Verwendung des Administratorkontos aus.
- **Neu starten:** Erteilt die Berechtigung, das Gerät neu zu starten.

- **Remotesteuerungseinstellungen angeben:** Dient der Einrichtung und Konfiguration von Berechtigungen für Benutzer der Remotesteuerung. Für das Ersuchen von Berechtigungen zur Ausführung der verschiedenen Befehle, die die Remotesteuerung bietet, können benutzerdefinierte Meldungen erstellt werden.
    - **Inaktive Sitzung schließen nach:** Sorgt dafür, dass die Remotesitzung bei Inaktivität automatisch getrennt wird. Wird hier der Wert " 0" eingegeben, trennt die Konsole die Verbindung der Remotesitzung bei Inaktivität nicht automatisch.
    - **Endbenutzer erteilt Erlaubnis für Remotesteuerungssitzung:** Gibt einem Benutzer, der bei einem remote gesteuerten, verwalteten Gerät angemeldet ist, die Möglichkeit, die Anforderung zu bestätigen, bevor ihnen die Steuerung des verwalteten Geräts entzogen wird.
    - **Nur wenn Benutzer angemeldet ist:** Fordert den zurzeit angemeldeten Benutzer auf, die Berechtigung zur Remotesteuerung zu erteilen. Wenn niemand angemeldet ist, muss für die Remotesteuerung keine Berechtigung abgerufen werden.
    - **Um Erlaubnis bitten, alle Features gleichzeitig zu verwenden:** Lässt es zu, dass nur einmal pro Sitzung eine Erlaubnis eingeholt werden muss, statt dass eine Erlaubnis für jedes einzelne Feature gefordert wird (Dateiübertragung, remote Ausführung usw.). Wenn diese Kontrollkästchen ausgewählt ist, wird der Benutzer nur einmal während der Remotesteuerungssitzung um Erlaubnis gebeten, unabhängig davon, welche Prozesse ausgeführt werden.
    - **Benutzerdefinierte Meldung anzeigen:** Fordert den Benutzer mit einer hier erstellten, benutzerdefinierten Meldung auf, seine Erlaubnis für Folgendes zu geben:
        - Remotesteuerung
        - Chat
        - Remoteausführung
        - Dateiübertragung
        - Neustart
        - Alle Berechtigungen
    - **Meldungsfeld für Erlaubnis schließen nach:** Gibt dem Benutzer die Möglichkeit, die Erlaubnis für das verwaltete Gerät (innerhalb der angegebenen Sekunden) zu erteilen oder zu verweigern. Diese Einstellung ist konfigurierbar und legt fest, wie lange das Erlaubnisfenster bei der Anfrage, ob ein verwaltetes Gerät remote gesteuert werden darf, geöffnet bleibt.

Bereitstellen von LANDesk Sicherheitsdiensten

Der Sicherheitsscanner (d. h. der Patch und Compliance-Scanner) wird standardmäßig mit dem Standard LANDesk Agenten installiert. Sie müssen jedoch die Optionen der spezifischen Sicherheits- und Patchscanner-Seite verwenden, wenn Sie Geräteagentenkonfigurationen erstellen, um gewisse Aspekte über das Wie und Wann der Ausführung des Sicherheitsscanners auf den verwalteten Geräten zu konfigurieren. Darüber hinaus können Sie Einstellungen aktivieren und konfigurieren, mit denen benutzerdefinierte Variablen außer Kraft gesetzt werden, und Sie können häufige Sicherheitsscans sowie Echtzeit-Spyware- und Anwendungsblockierung aktivieren und konfigurieren.

Mit dem Sicherheitsscanner können Sie verwaltete Geräte auf bekannte Betriebssystem- und Anwendungsanfälligkeiten und andere Sicherheitsrisiken, wie z. B. Spyware, Viren, nicht genehmigte Anwendungen, Software- und Treiberupdates, Systemkonfigurations-Sicherheitsbedrohungen, benutzerdefinierte Sicherheitsdefinitionen usw. durchsuchen. Der Inhalt Ihres Sicherheitsscans variiert in Abhängigkeit von Ihrem Security Suite Inhaltsabonnement und wird zudem davon bestimmt, welche Sicherheitstypdefinitionen Sie heruntergeladen haben. Darüber hinaus können Sie erkannte Probleme mit der Funktionen "Automatisches Korrigieren" sowie mithilfe von Reparaturtasks und Richtlinien reparieren. Einzelheiten zu diesen Verfahren finden Sie unter "Patch und Compliance" auf Seite 578.

Weiter unten finden Sie Informationen zu den folgenden die Sicherheit betreffenden Seiten: Klicken Sie auf eine Verknüpfung, um zu diesem Abschnitt zu wechseln.

- "Informationen zur Seite "Patch- und Compliancescan"" auf Seite 134
- "Informationen zur Seite "Benutzerdefinierte Variablen"" auf Seite 135
- "Informationen zur Seite "Häufig ausgeführter Sicherheitsscan"" auf Seite 136
- "Die Seite "LANDesk Antivirus"" auf Seite 137
- "Informationen zur Seite "Spyware"" auf Seite 138
- "Informationen zur Seite "Anwendungsblocker"" auf Seite 138
- "Informationen zur Seite "Windows-Firewall"" auf Seite 139
- "Informationen zur Seite "Endpunktsicherheit"" auf Seite 139
- "Informationen zur Seite "Agentenüberwachung"" auf Seite 140
- "Informationen zur Seite "LANDesk 802.1x-Unterstützung"" auf Seite 140
- "Informationen zur Seite "Erweiterte Geräteerkennung"" auf Seite 142

Informationen zur Seite "Patch- und Compliancescan"

Diese Seite verwenden Sie, um festzulegen, wie der Sicherheitsscanner (d. h. der Patch- und Compliancescan) gestartet wird und wie er sich auf verwalteten Geräten, die über diese Agentenkonfiguration verfügen, verhält.

HINWEIS: Sicherheitsscans lassen sich auch als geplante Tasks und Richtlinien von der Konsole aus oder manuell auf einem verwalteten Gerät ausführen.

Diese Seite enthält folgende Optionen:

- **Ereignisgesteuerter Scan:**
  - **Wenn sich der Benutzer anmeldet:** Fügt den Sicherheitsscanner in den Run-Key der Windows-Registrierung ein. Hiermit wird veranlasst, dass der Scanner immer dann ausgeführt wird, wenn auf den verwalteten Geräten, die über diese Agentenkonfiguration verfügen, eine Anmeldung erfolgt.

- **Zeitplangesteuerter Scan:**
  - **Einstellungen ändern:** Öffnet das Dialogfeld **Sicherheits- und Patchscan planen**. In diesem Dialogfeld können Sie Zeitplaneinstellungen für Sicherheitsscans konfigurieren, die vom Local Scheduler gestartet werden. Der Local Scheduler startet sobald wie möglich (innerhalb des von Ihnen angegebenen Zeitraums und basierend auf den von Ihnen festgelegten Beschränkungen) einen regelmäßig wiederkehrenden Sicherheitsscan. Sie können ferner Optionen für die Ausführung des Sicherheitsscanners konfigurieren, wenn bei einem Gerät bestimmte Bedingungen erfüllt sind, wie zum Beispiel: Nur wenn ein Benutzer angemeldet ist, nur wenn eine bestimmte Mindestbandbreite zur Verfügung steht und sobald sich die IP-Adresse eines Geräts ändert. Nachdem Sie diese Zeitplaneinstellungen für den Sicherheitsscanner konfiguriert haben, klicken Sie ganz einfach auf **Speichern**, um zur Hauptseite zurückzukehren (dort werden jetzt die Zeitplankriterien angezeigt).
- **Globale Einstellungen:** Gilt für alle Geräte, die über diese Agentenkonfiguration verfügen; die Option überschreibt taskspezifische Einstellungen.
  - **Nie neu starten:** Stellt sicher, dass Geräte, die über diese Agentenkonfiguration verfügen, während der Ausführung des Sicherheitsscanners nicht neu gestartet werden. Es handelt sich hierbei um eine globale Einstellung für alle Geräte, die über diese Agentenkonfiguration verfügen; d. h., die Einstellung überschreibt alle Endanwender-Neustarteinstellungen, die auf einen Sicherheitsscan oder Reparaturtask angewendet werden. Mit anderen Worten, diese Einstellung hat immer Priorität, ganz gleich, welche Endanwender-Neustarteinstellungen von einem Sicherheitsscan verwendet werden. Aktivieren Sie diese Option, wenn Sie verhindern möchten, dass Geräte während eines Sicherheitsscans neu gestartet werden, und markieren Sie die Option nicht, wenn Sie die Neustartoptionen mit dem Extra "Patch und Compliance" konfigurieren möchten.
  - **Automatisches Korrigieren nie verwenden:** Stellt sicher, dass Geräte, die über diese Agentenkonfiguration verfügen, nicht zulassen, dass ein Sicherheits- und Patchscan eine automatische Reparatur für erkannte Anfälligkeiten durchführt, selbst wenn für die Anfälligkeit die automatische Reparatur aktiviert wurde. Als globale Einstellung für alle Geräte, die über diese Agentenkonfiguration verfügen, überschreibt diese Einstellung alle Endanwender-Reparatureinstellungen, die Sie auf einen Sicherheitsscan-Task übertragen hatten. Verwenden Sie diese Einstellung, wenn Sie sicherstellen möchten, dass auf Geräten keine Möglichkeit besteht, erkannte Anfälligkeiten automatisch durch einen Sicherheitsscan reparieren zu lassen.
- **Scan- und Reparatureinstellungen:** Legt die vom Sicherheitsscanner auf verwalteten Geräten angezeigten Informationen, Endanwender-Interaktionen, Neuboot-Operation und Inhaltseinstellungen fest, wenn der Scanner auf verwalteten Geräten, die über diese Agentenkonfiguration verfügen, mit der oben ausgewählten Methode (Run Key während Anmeldung, Local Scheduler oder beides) gestartet wird. Wählen Sie eine Scan- und Reparatureinstellung aus der Dropdownliste aus, um sie auf die Konfiguration anzuwenden, die Sie gerade erstellen. Sie können auch auf **Konfigurieren** klicken, um eine neue Scan- und Reparatureinstellung zu erstellen und anzuwenden oder eine vorhandene zu bearbeiten.

Informationen zur Seite "Benutzerdefinierte Variablen"

Verwenden Sie diese Seite, um eine Einstellung zur Außerkraftsetzung einer benutzerdefinierten Variablen Geräten zuzuordnen, die über diese Agentenkonfiguration verfügen.

Der Sicherheitsscanner kann benutzerdefinierte Variablen (editierbare Werte, die in bestimmten Sicherheitstyp-Definitionen enthalten sind) verwenden, um nach bestimmten Einstellungen zu suchen und sie zu ändern, und um Standard-Konfigurationseinstellungen auf verwalteten Geräten zu implementieren. Sie können den Wert einer Einstellung ändern und Sie können festlegen, ob der aktuelle Wert mit dem neuen Wert überschrieben werden soll. Anschließend können Sie dann mit dieser Agentenkonfiguration die Konfiguration auf Zielgeräte anwenden. In manchen Situationen sollten Sie eine benutzerdefinierte Variableneinstellung ggf. ignorieren oder – anders ausgedrückt – eine Ausnahme von der Regel erstellen. Mithilfe der Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen können Sie entscheiden, welche benutzerdefinierten Variablen beim Scannen von Geräten ignoriert werden, damit sie nicht als anfällig erkannt und repariert werden, selbst wenn sie eigentlich die Bedingungen der Erkennungsregeln einer Definition erfüllen.

Eine Einstellung zur Außerkraftsetzung für benutzerdefinierte Variablen wird bei einer Agentenkonfiguration nicht benötigt.

Sie können eine vorhandene Einstellung aus der Liste **Benutzerdefinierte Variableneinstellungen** auswählen, auf **Konfigurieren** klicken, um eine neue Einstellung zu erstellen, oder das Feld leer lassen.

Diese Seite enthält folgende Optionen:

- **Benutzerdefinierte Variableneinstellungen:** Gibt Einstellungen für die Außerkraftsetzung von benutzerdefinierten Variablen auf Zielgeräten an, wenn diese auf Sicherheitsdefinitionen durchsucht werden, die benutzerdefinierte Variablen enthalten (beispielsweise Sicherheitsbedrohungen und Viren). Mithilfe der Funktion "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen" können Sie Einstellungswerte angeben, die Sie während eines Sicherheitsscans ignorieren oder umgehen möchten. Dies ist eine äußerst nützliche Funktion, wenn Sie ein gescanntes Gerät NICHT als anfällig in Übereinstimmung mit den standardmäßigen benutzerdefinierten Variableneinstellungen identifizieren lassen möchten. Wählen Sie eine Einstellung aus der Liste aus. Über die Liste können Sie außerdem die Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen auf Zielgeräten entfernen. Mit der Option **Benutzerdefinierte Variableneinstellungen entfernen** können Sie die Einstellungen auf einem Gerät so festlegen, dass benutzerdefinierte Variableneinstellungen vollständig in Kraft sind. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählte Einstellung zu ändern. Klicken Sie auf **Konfigurieren**, um eine neue Einstellung zu erstellen. Weitere Informationen hierzu finden Sie unter "Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen"" auf Seite 685.

Informationen zur Seite "Häufig ausgeführter Sicherheitsscan"

Verwenden Sie diese Seite, um einen regelmäßig wiederkehrenden Sicherheitsscan für eine Sammlung von Anfälligkeiten mit hohem Risikopotenzial oder andere Sicherheitsdefinitionen auf Geräten mit dieser Agentenkonfiguration zu aktivieren und konfigurieren. Ein häufig ausgeführter Sicherheitsscan ist nützlich, wenn Sie Geräte in regelmäßigen Abständen auf besonders aggressive und destruktive Sicherheitsangriffe scannen müssen.

HINWEIS: Nur Gruppenscans
Die häufig ausgeführten Sicherheitsscans basieren auf den Sicherheitsdefinitionen, die in einer Gruppe enthalten sind, die Sie aus vordefinierten Sicherheitsinhaltsgruppen ausgewählt haben.

Diese Seite enthält folgende Optionen:

- **Häufig ausgeführten Sicherheitsscan verwenden:** Aktiviert einen häufig ausgeführten Sicherheitsscan auf Geräten mit dieser Agentenkonfiguration.

- **Nur Scannen, wenn Benutzer angemeldet ist:** Schränkt den häufigen Sicherheitsscan insofern ein, als dieser nur ausgeführt wird, wenn auf dem Zielgerät ein Benutzer angemeldet ist.
- **Alle:** Gibt das Zeitintervall für einen häufig ausgeführten Sicherheitsscan an.
- **Eine Scan- und Reparatureinstellung wählen:** Gibt die Scan- und Reparatureinstellungen an, die den Sicherheitsscanner für häufig ausgeführte Sicherheitsscans steuern. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten und wie sich die Interaktion mit den Benutzern gestaltet. Die von Ihnen ausgewählte Einstellung muss für das Scannen von Gruppen (nicht Typen) konfiguriert werden. Sie können auch auf **Konfigurieren** klicken, um eine neue Scan- und Reparatureinstellung zu erstellen, die mit einer Gruppe verknüpft ist.

Die Seite "LANDesk Antivirus"

Verwenden Sie diese Seite, um eine Antivirus-Einstellung auszuwählen, die für Geräte mit dieser Agentenkonfiguration gilt, und um festzulegen, ob vorhandene Antivirus-Produkte auf diesen Geräten beim Konfigurieren entfernt werden sollen.

HINWEIS: Diese Seite gilt NICHT für eine neue Windows Embedded Standard-Agentenkonfiguration.

Um eine Antivirus-Einstellung auswählen zu können, müssen Sie zunächst das Kontrollkästchen des LANDesk Antivirus-Agenten auf der Seite **Start** aktivieren.

Mithilfe von Virenschutzeinstellungen können Sie steuern, wie der Virenschutzscanner auf Zielgeräten ausgeführt wird. Sie können u. a. folgende Virenschutz-Scanparameter definieren: zu scannende oder auszuschließende Dateien und Ordner, Echtzeitscans, geplante Scans, Quarantäne- und Backupoptionen, Aktualisierungsoptionen für Virenmusterdateien und die Informationen und interaktiven Optionen, die auf dem Gerät des Endanwenders während der Ausführung eines Virenschutzscans angezeigt werden.

HINWEIS: Bereitstellen von LANDesk Antivirus auf Geräten, auf denen bereits ein Antivirusprodukt installiert ist
Wenn auf Zielgeräten bereits ein Antivirus-Produkt installiert ist, können Sie dieses Produkt während der Konfiguration des Agenten automatisch entfernen lassen; hierfür müssen Sie die Option **Vorhandenes Antivirusprodukt entfernen** auswählen. Wenn Sie festlegen, dass das andere Antivirus-Produkt während der Agentenkonfiguration nicht entfernt werden soll, bleibt LANDesk Antivirus so lange deaktiviert, bis Sie das andere Produkt manuell entfernen. Sie können den Dienst jedoch nach wie vor auf Zielgeräten bereitstellen.

Eine Liste mit den Antivirusprodukten, die von Geräten entfernt werden können, finden Sie unter "LANDesk Antivirus" auf Seite 751.

Diese Seite enthält folgende Optionen:

- **Vorhandenes Antivirus-Produkt entfernen:** Entfernt vor dem Installieren von LANDesk Antivirus automatisch andere Antivirus-Produkte, die möglicherweise bereits auf den Geräten installiert sind. (**HINWEIS:** Sie können vorhandene Antivirussoftware auf verwalteten Geräten auch bei der Erstellung eines Tasks zum **Installieren oder Aktualisieren von Antivirus** entfernen.)

- **LANDesk Antivirus-Einstellungen:** Mithilfe der Antivirus-Einstellungen können Sie die Anzeige des Antivirus-Symbols in der Symbolleiste des Geräts ein- oder ausschalten, die Verfügbarkeit von interaktiven Optionen für Endanwender steuern, die Einstellungen in Bezug auf die Aktivierung von E-Mail-Scans und Echtzeitschutz festlegen, die zu scannenden Dateitypen und auszuschließenden Dateien und Ordner auswählen, infizierte Dateien unter Quarantäne stellen, Backups veranlassen und die Durchführung geplanter Antivirusscans und Virendefinitionsdateiupdates konfigurieren. Wählen Sie eine Einstellung aus der Liste aus. Klicken Sie auf **Konfigurieren**, um eine neue Einstellung zu erstellen.

Informationen zur Seite "Spyware"

Verwenden Sie diese Seite zur Aktivierung der Spyware-Erkennung in Echtzeit und zur Benachrichtigung auf Geräten, die über diese Agentenkonfiguration verfügen.

Die Spyware-Erkennung in Echtzeit sucht nur nach Spyware-Definitionen, die sich in der Gruppe **Scannen** befinden und für die "Automatisches Korrigieren" eingeschaltet ist. Sie können die Option "Automatisches Korrigieren" für heruntergeladene Spyware-Definitionen entweder automatisch aktivieren oder Sie können Spyware-Definitionsupdates konfigurieren, sodass die Option "Automatisches Korrigieren" beim Download der Definitionen automatisch aktiviert wird.

Die Spyware-Erkennung in Echtzeit überwacht Geräte auf neu gestartete Prozesse, die versuchen, die lokale Registrierung zu manipulieren. Wenn Spyware erkannt wird, fordert der Sicherheitsscanner des Geräts den Endanwender auf, die Spyware zu entfernen.

Diese Seite enthält folgende Optionen:

- **Echtzeit-Spywareblockierung aktivieren:** Aktiviert Spyware-Überwachung und Blockierung in Echtzeit auf Geräten, die über diese Agentenkonfiguration verfügen.

  HINWEIS: Damit das Echtzeit-Spyware-Scanning und die Spyware-Erkennung funktioniert, müssen Sie die automatische Korrekturfunktion manuell aktivieren, um die heruntergeladenen Spyware-Definitionen im Sicherheitsscan einzuschließen. Die automatische Reparaturfunktion ist für heruntergeladene Spyware-Definitionen standardmäßig nicht eingeschaltet.

- **Benutzer benachrichtigen, wenn Spyware blockiert wurde:** Zeigt eine Meldung an, die den Endanwender informiert, dass ein Spyware-Programm erkannt und repariert wurde.
- **Wenn eine Anwendung nicht als Spyware erkannt wird, die Genehmigung des Benutzers für die Installation anfordern:** Selbst wenn der erkannte Prozess nicht als Spyware eingestuft wird (gemäß der aktuellen Liste der Spyware-Definitionen für dieses Gerät), wird der Benutzer dennoch zur Bestätigung aufgefordert, bevor die Software auf dem Computer installiert wird.

Informationen zur Seite "Anwendungsblocker"

Verwenden Sie diese Seite, um die Echtzeitblockierung und -benachrichtigung bei Verwendung nicht autorisierter Anwendungen zu aktivieren. Der Echtzeit-Anwendungsblocker sucht nur nach Anwendungen, die sich in der Gruppe Scannen befinden.

Bei Verwendung der Anwendungsblockierung in Echtzeit ist die Reparatur kein separater Task. Das Verweigern einer Anwendung findet als Teil des eigentlichen Sicherheitsscans statt, indem die Registrierung auf dem lokalen Festplattenlaufwerk so bearbeitet wird, dass der Benutzerzugriff auf diese nicht autorisierten Anwendungen deaktiviert wird. Die Sicherheitsdienste verwenden das Feature "softmon.exe", um den Zugriff auf spezifische Programmdateien zu verweigern, selbst wenn der Name der ausführbaren Datei geändert wurde, da softmon.exe die Dateiheader-Informationen liest.

Diese Seite enthält folgende Optionen:

- **Blockierung der unzulässigen Anwendungen aktivieren:** Aktiviert Anwendungsblockierung in Echtzeit auf Geräten, die über diese Agentenkonfiguration verfügen.
- **Benutzer benachrichtigen, wenn eine Anwendung blockiert wurde:** Zeigt eine Meldung an, die den Benutzer informiert, dass er versucht hat, eine unzulässige Anwendung zu starten, und dass der Zugriff verweigert wurde.

Informationen zur Seite "Windows-Firewall"

Verwenden Sie diese Seite, um die Windows-Firewall auf verwalteten Geräten mit dieser Agentenkonfiguration zu aktivieren und konfigurieren. Hier können Sie die Firewall aktivieren/deaktivieren und Firewalleinstellungen konfigurieren, einschließlich Ausnahmen, Eingangsregeln und Ausgangsregeln (für Dienste, Ports und Programme).

Sie können diese Funktion verwenden, um eine Konfiguration für die Windows-Firewall auf den folgenden Windows-Versionen bereitzustellen:

- Windows 2003
- Windows XP (SP2 oder neuer)
- Windows Vista

Diese Seite enthält folgende Optionen:

- **Windows-Firewall konfigurieren:** Aktiviert die automatische Konfiguration der Windows-Firewall auf Geräten mit dieser Agentenkonfiguration.
- **Windows-Firewalleinstellungen:** Gibt die Windows-Firewalleinstellungen an, die auf Zielgeräten bereitgestellt werden, die über diese Agentenkonfiguration verfügen. Wählen Sie eine Einstellung aus der Liste aus, um sie auf die Konfiguration anzuwenden, die Sie gerade erstellen. Sie können auch auf **Konfigurieren** klicken, um eine neue Scan- und Reparatureinstellung zu erstellen und anzuwenden oder eine vorhandene zu bearbeiten.

Informationen zur Seite "Endpunktsicherheit"

Diese Seite verwenden Sie, um Einstellungen für die Endpunktsicherheit für verwaltete Geräte mit dieser Agentenkonfiguration auszuwählen. Die Endpunktsicherheit umfasst drei Komponenten: HIPS, LANDesk Firewall und Gerätesteuerung.

Um eine Einstellung für die Endpunktsicherheit auswählen zu können, müssen Sie zunächst das Kontrollkästchen des Agenten für Endpunktsicherheit auf der Seite **Start** aktivieren.

Diese Seite enthält folgende Optionen:

- **Einstellungen für die Endpunktsicherheit:** Gibt die Einstellungen für die Endpunktsicherheit auf Zielgeräten mit dieser Agentenkonfiguration an. Die Einstellungen für die Endpunktsicherheit bestimmen die allgemeine Funktion der Endpunktsicherheit (wie z. B. Standorterkennung, Administratorkennwort, Stoppoption für Endbenutzer und Popup-Nachrichten) und welche

Sicherheitsrichtlinien für HIPS, LANDesk Firewall und die Gerätesteuerung bereitgestellt werden. Sie können auch auf **Konfigurieren** klicken, um eine neue Einstellung zu erstellen.

- **Konfiguration vom Core aus aktualisieren:** Gibt Ihnen die Möglichkeit, die Einstellungen für die Endpunktsicherheit auf Zielgeräten mit dieser Agentenkonfiguration zu aktualisieren.

Informationen zur Seite "Agentenüberwachung"

Verwenden Sie diese Seite, um die LANDesk Agentenüberwachung auf Geräten mit dieser Agentenkonfiguration zu aktivieren und konfigurieren.

Mit der Agentenüberwachung können Sie Geräte aktiv auf ausgewählte LANDesk Agentendienste und -dateien überwachen. Die Agentenüberwachung startet gestoppte Agentendienste neu und setzt die Starttypen für Dienste zurück, die auf automatisch festgelegt wurden. Um zu verhindern, dass Dateien gelöscht werden, entfernt das Dienstprogramm außerdem überwachte Agentendateien aus Listen, die beim Neustart zu löschende Dateien enthalten. Darüber hinaus benachrichtigt die Agentenüberwachung Sie, wenn Agentendienste nicht neu gestartet werden können, wenn Agentendateien gelöscht wurden und wenn Agentendateien planmäßig beim Neustart zu löschen sind.

Diese Seite enthält folgende Optionen:

- **Agentenüberwachung benutzen:** Aktiviert das Dienstprogramm "Agentenüberwachung" auf Geräten, die über diese Agentenkonfiguration verfügen.
- **Agentenüberwachungseinstellungen:** Gibt die Agentenüberwachungseinstellungen an, die auf Zielgeräten bereitgestellt werden, die über diese Agentenkonfiguration verfügen. Agentenüberwachungseinstellungen bestimmen, welche Dienste und Dateien wie oft überwacht werden und ob das Dienstprogramm auf dem Gerät verbleibt. Wählen Sie eine Einstellung aus der Liste aus. Klicken Sie auf **Konfigurieren**, um eine neue Einstellung zu erstellen.

Informationen zur Seite "LANDesk 802.1x-Unterstützung"

Diese Seite verwenden Sie, um die LANDesk 802.1x NAC-Lösung zu aktivieren. Sie können 802.1x dazu verwenden, Ihre Compliance-Sicherheitsrichtlinie auf verwalteten Geräten, die 802.1x unterstützen, durchzusetzen, indem Sie Scans ausführen, Zugriff je nach Zustand (Compliance) gewähren oder blockieren, fehlerhafte (non-compliant) Geräte unter Quarantäne stellen und Reparaturen durchführen.

HINWEIS: Aktivieren und Konfigurieren von 802.1x NAC mit einer Agentenkonfiguration
Damit Sie 802.1x NAC aktivieren und die Optionen auf dieser Seite konfigurieren können, müssen Sie zunächst im Extra "Network Access Control" im Dialogfeld "802.1x-Konfiguration" die Option **802.1x Radius-Server** auswählen (**Extras > Sicherheit > Network Access Control > 802.1x konfigurieren > Radius-Server**). Nachdem Sie diese Option ausgewählt haben, können Sie diese Seite zur Konfiguration von 802.1x mit einer Agentenkonfiguration verwenden.

Diese Seite enthält folgende Optionen:

- **LANDesk 802.1x-Unterstützung aktivieren:** Aktiviert 802.1x NAC auf Geräten, die über diese Agentenkonfiguration verfügen. 802.1x NAC verwendet den im Extra "NAC" definierten EAP-Typ. Die Einstellung für den EAP-Typ gilt für den gesamten Core. Mit anderen Worten: Alle mit dieser Agentenkonfiguration konfigurierten Geräte werden mit dem in der Konsole angegebenen EAP-Typ konfiguriert.
- **PEAP-Einstellungen konfigurieren:** Öffnet ein Dialogfeld, in dem Sie die Einstellungen für den Server und die vertrauenswürdige Zertifizierungsstelle festlegen.

- **Quarantänenetzwerkadresse:**
  - **IP in selbstzugewiesenem Bereich verwenden:** Gibt an, dass für fehlerhaft erklärte (non-compliant) Geräte aufgrund der Compliance-Sicherheitsrichtlinie mithilfe der eingebauten, selbst zugewiesenen IP-Adressenbereichsfunktion des TCP/IP-Protokolls in ein Quarantänenetzwerk gesendet werden.
  - **DHCP im Quarantänenetzwerk verwenden:** Gibt an, dass Geräte, die basierend auf der Compliance-Sicherheitsrichtlinie für fehlerhaft (non-compliant) erklärt wurden, mittels eines DHCP-Servers und Wartungsservers, den Sie in Ihrem Netzwerk konfiguriert haben, in ein Quarantänenetzwerk gesendet werden.
    - **Wählen Sie den primären Wartungsserver aus:** Gibt den Reparaturserver an, den Sie zur Reparatur von fehlerhaften Geräten verwenden möchten, damit sie wieder gescannt werden und Zugang zum Unternehmensnetzwerk erhalten können.
    - **Wartungs-Sicherungsserver:** Gibt Ihnen die Möglichkeit einen Sicherungsserver für die Wartung zu konfigurieren, für den Fall, dass ein Zugriff auf den primären Wartungsserver nicht möglich ist. Klicken Sie auf **Konfigurieren**, um einen Wartungsserver hinzuzufügen.
- **Client unter Quarantäne stellen, wenn innerhalb des folgenden Zeitrahmens keine Zustandsprüfung erfolgt ist:** Mit dieser Option automatisieren Sie die Gerätequarantäne, indem Sie eine maximale Zeitspanne angeben, in der ein Gerät als fehlerfrei angesehen werden kann, ohne dass ein Compliance-Sicherheitsscan darauf ausgeführt wurde. Wenn diese Zeitspanne ohne Scannen überschritten wird, wird das Gerät automatisch ins Quarantänenetzwerk gestellt.

Bereitstellen des Schreibfilters für Windows Embedded-Standardgeräte

Verwenden Sie diese Option, um einen bestimmten Zeitraum zu definieren, während dem der LANDesk Administrator und/oder vom Administrator erstellte geplante Tasks und Richtlinien Schreibvorgänge auf einem verwalteten Gerät mit dem Windows Embedded-Standardbetriebssystem durchführen können.

WICHTIG: NUR für HP Thin Client WES-Geräte
Diese Option steht NUR für HP Thin Client-Geräte mit Windows Embedded Standard (WES 7 und WES 09) Betriebssystem zur Verfügung.

Das Schreibfilterfenster für das Embedded-Betriebssystem gibt den Zeitraum an, während dem das verwaltete Gerät das Schreiben von Daten auf seine Festplatte zulässt. Zu Beginn dieses "Wartungsfensters" wird der Schreibfilter deaktiviert und das Gerät wird neu gestartet. Anschließend werden die angewendeten Richtlinien, Tasks und Prozesse auf dem Gerät ausgeführt. Je nach den zugewiesenen Richtlinien kann dies innerhalb kurzer Zeit erledigt sein oder aber auch etwas mehr Zeit in Anspruch nehmen. Nach Abschluss aller Richtlinien und Prozesse (bzw. wenn eine Endzeit definiert wurde: sobald die Endzeit des "Wartungsfensters" erreicht ist) wird der erweiterte oder dateibasierte Schreibfilter entsprechend dem vorherigen Zustand erneut aktiviert und das Gerät neu gestartet.

Sie können entweder unbefristet Zeit einräumen, damit alle Richtlinien und Prozesse abgeschlossen werden können, oder Sie können eine bestimmte Endzeit angeben, bei der alle aktiven Vorgänge eingestellt werden und das Gerät automatisch neu gestartet wird, unabhängig davon, ob zu diesem Zeitpunkt ein Prozess ausgeführt wird oder nicht. Die Option **Endzeit** ist eine Sicherheits- bzw. Vorsichtsmaßnahme, die verhindern soll, dass das Gerät für längere Zeit unberechtigtem Zugriff ausgesetzt ist. Sie müssen jedoch im Hinblick auf die Zeit für ein entsprechendes Gleichgewicht sorgen, damit die erforderlichen Richtlinien abgeschlossen werden können, ohne dass es dabei zu einer Gefährdung des Status oder Zustands des verwalteten Geräts kommt.

VORSICHT: Wenn Sie eine bestimmte Endzeit für die Aktivierung des Schreibfilters und die Ausführung von Richtlinien und Prozessen definieren, denken Sie daran, dass es zu einem Verlust oder zur Beschädigung von Daten kommen kann, wenn beim Erreichen der Endzeit nicht alle Prozesse abgeschlossen werden konnten. Sie müssen daher den Zeitbedarf für die Durchführung und den Abschluss aller angewendeten Richtlinien und Task genau abschätzen und festlegen. Oder aber Sie definieren KEINE Endzeit.

Informationen zur Seite "Schreibfilter des Embedded-Betriebssystems"

Diese Seite enthält folgende Optionen:

- **Fenster:** Gibt das Zeitfenster an, während dem auf das Zielgerät geschrieben werden kann.
- **Startzeit:** Gibt den genauen Zeitpunkt an, zu dem mit dem Schreiben auf das Gerät begonnen werden kann.
- **Aktivierte Wochentage:** Gibt die Wochentage an, an denen Schreibvorgänge stattfinden können.
- **Geben Sie eine Endzeit für das Schreibfilterzeitfenster ein:** Aktivieren Sie diese Option, wenn Sie das Gerät zwingen möchten, Schreibvorgänge ab einem bestimmten Zeitpunkt nicht zuzulassen, indem der Schreibfilter (entweder der erweiterte oder der dateibasierte Schreibfilter) wieder aktiviert wird und unmittelbar zu dem als Endzeit festgelegten Zeitpunkt ein Neustart erfolgt.
- **Endzeit:** Gibt den genauen Zeitpunkt an, zu dem jegliche Schreibvorgänge auf dem Gerät gemäß dem oben beschriebenen Verfahren beendet werden.

WARNUNG: Die Angabe einer Endzeit für das Schreibfilterfenster bewirkt einen sofortigen Neustart beim Erreichen dieses Zeitpunkts und das Gerät wird wieder in einen Zustand mit aktiviertem Schreibfilter versetzt, unabhängig davon, ob Richtlinien und Tasks abgeschlossen wurden oder nicht.

Bereitstellung der erweiterten Geräteerkennung

Die erweiterte Geräteerkennung stellt eine Erweiterung des Extras "Erkennung nicht verwalteter Geräte" dar. Sie findet Geräte in Ihrem Netzwerk, die noch keinen Inventarscan an die Coredatenbank gesendet haben. Mit der erweiterten Geräteerkennung können Sie eine oder beide der folgenden Erkennungsmethoden verwenden: ARP-Erkennung (Address-Resolution-Protocol) und WAP-Erkennung (Wireless Access Point).

Informationen zur Seite "Erweiterte Geräteerkennung"

Diese Seite verwenden Sie, um die erweiterte Geräteerkennung auf verwalteten Geräten mit dieser Agentenkonfiguration zu aktivieren und konfigurieren.

Mit der ARP-Erkennung hört der Agent der erweiterten Geräteerkennung ARP-Broadcasts im Netzwerk ab. Der Agent prüft alle ARP-erkannten Geräte, um festzustellen, ob darauf der Standard LANDesk Agent installiert ist. Wenn der LANDesk Agent nicht reagiert, wird das ARP-erkannte Gerät in der Computerliste angezeigt. Die erweiterte Geräteerkennung leistet optimale Dienste in Situationen, in denen Firewalls Geräte daran hindern, auf die normalen pinggestützte UDD-Erkennungsmethoden zu antworten.

Denken Sie daran, dass Sie die erweiterte Geräteerkennung nicht auf jedem verwalteten Gerät in Ihrem Netzwerk bereitstellen müssen. Sie können es jedoch tun, wenn Sie es wünschen. Die Bereitstellung dieses Agenten auf mehreren Geräten in jedem Ihrer Subnetze sollte ausreichend sein.

Diese Seite enthält folgende Optionen:

- **Address-Resolution-Protocol (ARP) verwenden:** Aktiviert die erweiterte Geräteerkennung mithilfe der ARP-Erkennungsmethode (Address-Resolution-Protocol) auf Geräten mit dieser Agentenkonfiguration.
- **ARP-Erkennungseinstellung auswählen:** Gibt die ARP-Einstellung an, die den erweiterten Geräteerkennungsagenten steuert, wenn eine ARP-Erkennung in Ihrem Netzwerk durchgeführt wird. ARP-Einstellungen legen fest, wie oft der Erkennungsscan durchgeführt wird und auf welcher Protokollierungsebene. Wählen Sie eine Einstellung aus der Liste aus, um sie auf die Konfiguration anzuwenden, die Sie gerade erstellen. Sie können auch auf **Konfigurieren** klicken, um eine neue Einstellung zu erstellen und anzuwenden oder eine vorhandene zu bearbeiten.
- **Wireless Access Point (WAP)-Erkennung verwenden:** Aktiviert die erweiterte Geräteerkennung mithilfe der WAP-Erkennungsmethode (Wireless Access Point) auf Geräten mit dieser Agentenkonfiguration.
- **WAP-Erkennungseinstellung auswählen:** Gibt die WAP-Einstellung an, die den erweiterten Geräteerkennungsagenten steuert, wenn eine WAP-Erkennung in Ihrem Netzwerk durchgeführt wird. WAP-Einstellungen legen fest, wie oft der Erkennungsscan durchgeführt wird und auf welcher Protokollierungsebene. Wählen Sie eine Einstellung aus der **Dropdown**liste aus, um sie auf die Konfiguration anzuwenden, die Sie gerade erstellen. Sie können auch auf **Konfigurieren** klicken, um eine neue Einstellung zu erstellen und anzuwenden oder eine vorhandene zu bearbeiten.
- **Häufigkeit der Konfigurationsdownloads (in Minuten):** Gibt an, wie oft verwaltete Geräte, die über den Agenten der erweiterten Geräteerkennung verfügen, auf dem Coreserver nach einer aktualisierten Konfiguration der erweiterten Geräteerkennung suchen. Der Agent synchronisiert seine Konfiguration mit dem Core, wenn er zum ersten Mal geladen wird. Der Standardwert ist 720 Minuten (12 Stunden). Wenn Sie den Wert zu hoch setzen, dauert es einige Zeit, bis Konfigurationsänderungen auf Geräten übernommen werden. Setzen Sie ihn hingegen zu niedrig, dann ist die Belastung auf dem Core und im Netzwerk ggf. zu hoch.

Bereitstellen der Energieverwaltung

Die Funktionen der LANDesk Energieverwaltung ermöglichen die Erstellung, finanzielle Bewertung und Bereitstellung von Richtlinien zur Energieverwaltung und versetzen damit Administratoren in die Lage, den Energieverbrauch von Endknoten zentral zu steuern.

Informationen zur Seite "Energieverwaltung"

Die Seite **Energieverwaltung** verwenden Sie, um die Energierichtlinie auszuwählen, die an das Clientgerät verteilt werden soll. Während Administratoren zentral die Bedingungen steuern, unter denen Computer und Monitore in den Standby- oder Ruhezustand wechseln oder herunterfahren, können Benutzer bei Bedarf bestimmte Energieverwaltungsaktionen auf der Clientseite verhindern. Darüber hinaus schützt eine Option für ein weiches Herunterfahren ("Soft" Shutdown) vor dem Verlust nicht gespeicherter Daten. Eine vorab mit OEM Stromverbrauchsdaten gefüllte Datenbank wird mit den Istwerten des vorhandenen Hardwareinventars abgeglichen. Die verfügbaren benutzerdefinierten Stromverbrauchseinstellungen sorgen für hohe Genauigkeit bei der Ermittlung von Schätzwerten für die finanziellen Einsparungen und Stromeinsparungen.

Das Fenster "Energieverwaltung" enthält die folgenden Funktionen:

- **Energierichtlinie für den Client verwenden** Aktiviert die Energieverwaltung in dieser Agentenkonfiguration.
- **Energierichtlinien-Einstellungen:** Dient der Auswahl einer Energierichtlinie, die für den Einsatz auf verwalteten Geräten erstellt und konfiguriert wurde.

- **Wählen Sie eine Energierichtlinie aus:** Gibt die Energierichtlinie an, die mit der Agentenkonfiguration versendet wird. Standardmäßig steht eine oder keine Energierichtlinie zur Verfügung.
- **Clientverwendungsdaten sammeln:** Sammelt Stromverbrauchsdaten auf der Basis der Verwendung der einzelnen Clients. Diese Informationen werden dazu verwendet, genauere Berichte zum Stromverbrauch zu erstellen, und den exakten Strombedarf der verwalteten Geräte und der an sie angeschlossenen Monitore zu bestimmen.
- **Konfigurieren:** Hiermit können Sie Energieverwaltungsprofile erstellen, bearbeiten, kopieren oder löschen.

Bereitstellen von Desktop Manager

Desktop Manager stellt eine konsolidierte Desktop-Clientbenutzeroberfläche bereit, die über einen einzigen Shortcut im Startmenü sowohl Zugriff auf das Softwarebereitstellungsportal als auch auf die LaunchPad-Konsole gibt und damit die Benutzerfreundlichkeit entscheidend erhöht.

Informationen zur Seite "Desktop Manager"

Die **Desktop Manager**-Seiten verwenden Sie, um das Erscheinungsbild von Desktop Manager zu konfigurieren.

Diese Seite enthält folgende Optionen:

- **Verfügbare Anwendungen:** Listet die Anwendungen auf, die so konfiguriert werden können, dass der Zugriff über Desktop Manager möglich ist. Zu den Verfügbare Anwendungen gehören:
  - **LaunchPad:** Eine Konsole, die Zugriff auf Pakete, ausführbare Dateien, URLs und Process Manager-Links gibt, die spezielle für ein verwaltetes Gerät konfiguriert wurden. LaunchPad gewährt mit einem Mausklick Zugriff auf lokale, gehostete oder "Just-in-Time"-Anwendungen, die erst installiert werden, wenn ein Endbenutzer auf das Symbol klickt.
  - **Softwarebereitstellungsportal:** Zeigt alle Softwareverteilungspakete an, die mittels einer optionalen oder empfohlenen richtlinienbasierten Verteilungsmethode bereitgestellt wurden.
- **In Desktop Manager anzeigen:** Zeigt die Anwendungen an, die in Desktop Manager angezeigt werden und auf die über Desktop Manager zugegriffen werden kann. Verwenden Sie die Schaltflächen >> und <<, um die gewünschten Anwendungen auszuwählen. Standardmäßig sind sowohl LaunchPad als auch das Softwarebereitstellungsportal enthalten.

Informationen zur Seite "Anpassung" (unter Desktop Manager)

Die Seite **Anpassung** verwenden Sie, um die Shortcutspeicherorte für Desktop Manager auszuwählen sowie die Einstellungen für den Start und das Herunterfahren zu konfigurieren.

Die Seite **Anpassung** umfasst die folgenden Funktionen:

- **LANDesk Programmgruppe:** Erstellt ein Startmenü in der LANDesk Programmgruppe.
- **Windows-Desktop:** Erstellt einen Shortcut auf dem Desktop.
- **Windows-Startmenü:** Erstellt einen Eintrag im Startmenü.
- **Desktop Manager bei der Anmeldung des Benutzers ausführen:** Führt automatisch Desktop Manager aus, wenn sich der Benutzer beim verwalteten Gerät anmeldet.
- **Schließen von Desktop Manager nicht zulassen:** Verhindert, dass Benutzer das Fenster "Desktop Manager" schließen.

Informationen zur Seite "Branding" (unter Desktop Manager)

Die Seite **Branding** verwenden Sie, um den Inhalt und das Aussehen von Desktop Manager anzupassen.

Die Seite **Branding** umfasst die folgenden Funktionen:

- **Anwendungstitel:** Ermöglicht die Anpassung des Fenstertitels der Anwendung. Der Standardwert lautet "LANDesk Desktop Manager".
- **Ihre Meldung:** Gibt einem Administrator die Möglichkeit, eine angepasste Meldung unten zentriert im Desktop Manager-Fensters anzuzeigen. Standardmäßig wird keine Meldung angezeigt.
- **Unternehmenssymbol:** Hier können Sie eine Datei mit Ihrem Unternehmenssymbol hinzufügen, mit dem das Standardsymbol in Desktop Manager ersetzt wird. Das ausgewählte Symbol erscheint in der oberen linken Ecke neben "Softwarebereitstellungsportal”.
- **Unternehmenslogo:** Dient zum Hinzufügen eines Unternehmenslogos, das in der unteren linken Ecke des Fensters angezeigt wird. Das LANDesk Logo wird stets in der unteren rechten Ecke angezeigt.

Verwenden des Agentenkonfigurationstools

Informationen zum Dialogfeld "Agentenkonfigurationstool"

Das Dialogfeld **Agentenkonfigurationstool** zeigt den Status eines geplanten Gerätekonfigurationstasks während der Verarbeitung an. Es dient nur Ihrer Information. Die zu konfigurierenden Geräte wurden bereits bei der Planung des Tasks ausgewählt.

Das Dialogfeld **Agentenkonfigurationstool** enthält die folgenden Funktionen:

- **Zu konfigurierende Clients:** Führt die Geräte auf, die die Konfigurationseinstellungen erhalten sollen.
- **Clients, die konfiguriert werden:** Führt die Geräte auf, die von der Konsole kontaktiert wurden und die gerade mit dieser Einstellungsdatei konfiguriert werden.
- **Konfigurierte Clients:** Führt die Geräte auf, die die Konsole während dieser geplanten Sitzung konfiguriert hat. Wenn der Konfigurationsversuch erfolgreich war, ist der Status "Abgeschlossen". Falls der Konfigurationsversuch - aus welchem Grund auch immer - misslingt, lautet der Status "Fehlgeschlagen". Diese Statusangaben werden auch im Fenster "Geplante Tasks" angezeigt, wenn der entsprechende Task ausgewählt wird.
- **Konfigurationsdateien werden erstellt:** Zeigt eine Statusleiste mit dem Abschlussstatus des kompletten Konfigurationstasks an.

Informationen zum Dialogfeld "Bare Metal Server hinzufügen"

Mit dem Dialogfeld **Bare Metal Server hinzufügen** können Sie Geräte der Warteschlange hinzufügen, damit auf ihnen Versorgungstasks ausgeführt werden können. Diese Lösung ist besonders für die erste Bereitstellung auf neuen Geräten nützlich. Geräte werden der Warteschlange mithilfe eines Bezeichners hinzugefügt. Ein Serverbezeichner oder eine Serverkennung ist eine Informationseinheit, die dazu verwendet werden kann, einen Server eindeutig zu identifizieren. Ein Serverbezeichner kann eine MAC-Adresse (am gebräuchlichsten), die Seriennummer eines Anbieters, eine IPMI GUID oder eine vPro GUID sein. Der Bezeichner muss in jedem Fall von einem Agenten, der in der Prebootumgebung auf dem Zielserver ausgeführt wird, abgefragt werden können.

Sie können Geräte einzeln oder als Gruppen hinzufügen. Wenn Sie eine große Zahl von Geräten hinzufügen, müssen Sie eine Textdatei im CSV-Format mit Daten für die Geräte erstellen. Sie importieren diese Datei dann, um die Geräte zur Warteschlange hinzuzufügen.

So fügen Sie ein einzelnes Gerät hinzu

1. Erweitern Sie die Gruppe **Konfiguration** in der **Netzwerkansicht**. Klicken Sie mit der rechten Maustaste zunächst auf **Bare Metal Server** und dann auf **Geräte hinzufügen**.
2. Klicken Sie auf **Hinzufügen**. Geben Sie einen beschreibenden Namen in das Textfeld **Name** ein. Obwohl der Anzeigename wahlweise zu verwenden ist, ist er äußerst empfehlenswert. Auf einem Bare-Metal-Gerät ist der Anzeigename das einzige Unterscheidungsmerkmal in der Versorgungsansicht.
3. Wählen Sie einen Bezeichnertyp aus der Liste **Bezeichnertyp** aus (eine Mac-Adresse, Seriennummer, IPMI GUID oder Intel vPro GUID) und geben Sie den Wert in das Textfeld **Bezeichner** ein. Klicken Sie auf **Hinzufügen**.
4. Wiederholen Sie die Schritte 2 bis 3, um weitere Geräte hinzuzufügen. Sie können auch andere Bezeichner für das Gerät hinzufügen. Sie müssen lediglich einen weiteren Bezeichner mit denselben Anzeigenamen hinzufügen.
5. Klicken Sie auf **OK**.

So fügen Sie mehrere Geräte hinzu

1. Erweitern Sie die Gruppe **Konfiguration** in der **Netzwerkansicht**. Klicken Sie mit der rechten Maustaste zunächst auf **Bare Metal Server** und dann auf **Geräte hinzufügen**.
2. Wählen Sie in der Liste **Bezeichnertyp** eine Bezeichnertyp aus, der den Daten entspricht, die Sie importieren werden.
3. Geben Sie den Speicherort einer Textdatei (CSV), die die Informationen zum Bezeichner enthält, in das Textfeld ein (oder klicken Sie auf **Durchsuchen**, um die Datei ausfindig zu machen). Klicken Sie anschließend auf **Importieren**.

Jeder Bezeichner sollte durch ein Komma in der CSV-Datei getrennt werden. Das Importdateiformat ist Anzeigename, Kennung.

Bereitstellen von Agentenkonfigurationen für Linux- und UNIX-Server

Mit dem Extra "Agentenkonfiguration" der Konsole können Sie Agenten auf folgenden unterstützten Linux- und UNIX-Betriebssystemversionen bereitstellen: Weitere Informationen zur Bereitstellung von Linux-Agenten finden Sie unter "Konfigurieren von Linux- und UNIX-Geräteagenten" auf Seite 118.

Informationen zur Startseite (unter "Linux/UNIX-Agentenkonfiguration")

Die Seite **Start** der Linux-Agentenkonfiguration enthält die folgenden Optionen:

- **Konfigurationsname:** Geben Sie einen Namen ein, der die Konfiguration beschreibt, an der Sie zurzeit arbeiten. Dies kann ein bereits vorhandener oder ein neuer Konfigurationsname sein. Dieser Name wird im Fenster **Agentenkonfiguration** angezeigt.
- **Standard LANDesk Agent**, **Remotesteuerung** und **Softwareverteilung**: Diese Optionen werden standardmäßig installiert und können von Ihnen nicht deaktiviert werden.
- **LANDesk Anfälligkeitsscanner:** Installiert die Linux-Version des Anfälligkeitsscanners. Der Scanner meldet Probleme, repariert sie jedoch nicht.
- **Echtzeitinventar und Überwachung:** Installiert eine Agenten, der Echtzeitinventar und Überwachung über die LANDesk Management Console unterstützt.
- **Standardwerte:** Setzt die Optionen auf den jeweiligen Standardwert zurück (deaktiviert die Option **LANDesk**Anfälligkeitsscanner).

Informationen zur Seite "Standard LANDesk Agent" (unter "Linux/UNIX-Agentenkonfiguration")

Die Seite **Standard LANDesk Agent** der Linux-Agentenkonfiguration umfasst die folgenden Optionen:

- **Vertrauenswürdige Zertifikate für Agentenauthentifizierung:** Die Zertifikate bestimmen, welche Coreserver Geräte verwalten dürfen. Aktivieren Sie die Coreserver-Zertifikate, die mit dieser Konfiguration installiert werden sollen. Weitere Informationen finden Sie unter "Agentensicherheit und vertrauenswürdige Zertifikate" auf Seite 114.
- **HINWEIS:** Die anderen Optionen auf dieser Seite sind abgeblendet und gelten nicht für Linux-Agentenkonfigurationen.

Informationen zur Seite "Inventarscanner" (unter "Linux/UNIX Agentenkonfiguration")

Die Seite **Inventarscanner** der Linux-Agentenkonfiguration bietet die folgenden Optionen:

- **Inventarscan starten:** Sie können **täglich, wöchentlich oder monatlich** auswählen. Die von Ihnen ausgewählte Option fügt der cron.daily-, cron.weekly- oder cron.monthly-Datei des Servers einen Befehl hinzu, der den Inventarscanner ausführt.

Agentenüberwachung

Agentenüberwachung – Übersicht

Mit dem Extra „Agentenüberwachung“ können Sie den Status ausgewählter LANDesk Management Suite-Agentendienste und -Dateien proaktiv überwachen. Auf diese Weise können Sie sich jederzeit von der Integrität dieser Dienste und Dateien überzeugen und sicherstellen, dass diese auf verwalteten Geräten wie vorgesehen arbeiten. Die eigentliche Agentenüberwachung und die zugehörigen Einstellungen können mithilfe einer Erstkonfiguration für Geräteagenten bereitgestellt werden. Sie können die Agentenüberwachung außerdem jederzeit aktualisieren, ohne eine vollständige Agentenkonfiguration durchführen zu müssen.

Die Agentenüberwachung überwacht nicht nur kritische Dienste und -Dateien, sondern übernimmt auch folgende Aufgaben für Sie: Reaktivieren beendeter Dienste, Zurücksetzen von Diensten auf automatischen Start, Wiederherstellen von zu löschenden Dateien beim Neustart und Rückmeldung an den Coreserver bei begründetem Verdacht auf Dateimanipulation.

Die Agentenüberwachung überwacht die in den Agentenüberwachungseinstellungen eines Geräts angegebene LANDesk Management Suite-Dienste und -Dateien.

Mithilfe der Agentenüberwachungseinstellungen legen Sie außerdem fest, wie oft der Status von Agentendiensten und -Dateien überprüft werden soll, ob die Agentenüberwachung resident in den Speicher des Geräts geladen wird und ob die zugewiesenen Einstellungen selbst ebenfalls auf Änderungen überprüft werden soll.

Die Agentenüberwachung ist standardmäßig deaktiviert. Sie können die Agentenüberwachung mit einer Agentenkonfiguration oder (zu einem späteren Zeitpunkt) mit einem separaten Task der Kategorie "Agentenüberwachungseinstellungen aktualisieren" aktivieren. Mit anderen Worten: Sie müssen die Agentenüberwachung nicht beim erstmaligen Konfigurieren eines Geräts aktivieren. Sie können das Aktivieren jederzeit direkt von Konsole aus für verwaltete Geräte nachholen.

Beim Überwachen von Diensten und Dateien führt die Agentenüberwachung die unten aufgeführten Aktionen aus.

Unterstützte Geräteplattformen und Systemanforderungen

Die Agentenüberwachung unterstützt dieselben Plattformen, die auch von Management Suite unterstützt werden. Dazu zählen die folgenden Betriebssysteme, die mit den jeweiligen Mindestanforderungen für Software und Hardware aufgeführt sind:

- **Microsoft Windows XP 64 Bit Professional**
  (Intel Pentium 64 Bit-Prozessor oder kompatibles Gerät; 128 MB RAM empfohlen; für die Installation 72 MB auf Festplatte)
- **Windows 2000 Professional**
  (ab SP2; 133 MHz Intel Pentium-Prozessor oder kompatibles Gerät; 96 MB RAM, 96 MB empfohlen; für die Installation 50 MB auf Festplatte)
- **Microsoft Windows XP Professional**
  (Microsoft Internet Service Pack 2.0 oder höher; 300 MHz Intel Pentium-Prozessor oder kompatibles Gerät; 128 MB RAM empfohlen; für die Installation 72 MB auf Festplatte)

Überwachen von Diensten und Dateien mit der Agentenüberwachung

Mit der LANDesk Agentenüberwachung können die nachstehend genannten Dienste und Dateien überwacht werden.

Überwachung von Diensten

Die folgenden Agentendienste können überwacht werden:

- Local Scheduler
- Antivirus
- Remotesteuerung
- Softwareüberwachung
- Targeted Multicast

VORSICHT: Nicht von Ihnen bereitgestellte Dienste sollten nicht für die Überwachung durch die Agentenüberwachung ausgewählt werden
Wählen Sie beim Konfigurieren von Agentenüberwachungseinstellungen keine Dienste aus, die von Ihnen nicht für die Installation auf Zielgeräten vorgesehen sind. Andernfalls erhält der Coreserver Alarmmeldungen für nicht installierte Dienste, die absichtlich nicht installiert wurden. Beachten Sie jedoch, dass selbst wenn ein nicht installierter Dienst für die Überwachung ausgewählt wird, keine Alarmmeldungen (die sich darauf beziehen, dass der Dienst sich nicht neu starten oder sein Starttyp sich nicht ändern lässt) gesendet werden.

Im Rahmen der Überwachung von Agentendiensten führt die Agentenüberwachung folgende Aktionen aus:

- Startet Dienste neu, wenn sie ausfallen (ein Mal)
- Ändert den Starttyp des Dienstes zurück in automatisch, wenn der Starttyp geändert wird
- Alarmiert den Coreserver, wenn Dienste nicht installiert sind
- Alarmiert den Coreserver, wenn Dienste sich nicht neu starten lassen
- Alarmiert den Coreserver, wenn der Starttyp eines Dienstes sich nicht zurück in automatisch ändern lässt.

Überwachung von Dateien

Die folgenden Dateien sind von der Überwachung ausgeschlossen:

- Ldiscn32.exe
- Vulscan.dll
- Vulscan.exe
- Sdclient.exe

Im Rahmen der Überwachung von Dateien führt die Agentenüberwachung folgende Aktionen aus:

- Entfernt Dateien aus der Registrierung, die beim Neustart planmäßig zu löschen sind
- Alarmiert den Coreserver, wenn die Dateien beim Neustart planmäßig zu löschen sind
- Alarmiert den Coreserver, nachdem die Dateien gelöscht wurden

Aktivieren und Konfigurieren der Agentenüberwachung

Das Dienstprogramm für die Agentenüberwachung wird zusammen mit dem Management Suite-Agenten installiert, wobei es jedoch standardmäßig deaktiviert ist.

Die Agentenüberwachung kann auf zweierlei Weise aktiviert werden: Im Rahmen der Erstkonfiguration eines Geräteagenten oder zu einem späteren Zeitpunkt mithilfe eines Tasks vom Typ "Agentenüberwachungseinstellungen aktualisieren".

Aktivieren der Agentenüberwachung auf Geräten

So aktivieren Sie die Agentenüberwachung beim Konfigurieren von Agenten

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Windows Agentenkonfiguration**.
3. Nachdem Sie die gewünschten Einstellungen für die Agentenkonfiguration festgelegt haben, klicken Sie auf die Gruppe **Sicherheit und Compliance** und dann auf **Agentenüberwachung**, um die entsprechende Seite im Dialogfeld zu öffnen.
4. Aktivieren Sie das Kontrollkästchen **Agentenüberwachung benutzen**.
5. Wählen Sie eine der Einstellungen aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können neue Einstellungen definieren oder vorhandene Einstellungen bearbeiten. Die angewendeten Einstellungen bestimmen, welche Dienste und Dateien wie oft überwacht werden und ob die ausführbare Agentenüberwachungsdatei resident in den Speicher überwachter Geräte geladen wird.
6. Legen Sie alle gewünschten Einstellungen für die Agentenkonfiguration fest und klicken Sie dann auf **Speichern**.

Wenn Sie die Agentenüberwachung zu einem späteren Zeitpunkt aktivieren oder Agentenüberwachungseinstellungen zu einem späteren Zeitpunkt aktualisieren möchten, können Sie dies direkt von der Konsole aus tun (für ein verwaltetes Gerät oder mehrere verwaltete Geräte gleichzeitig).

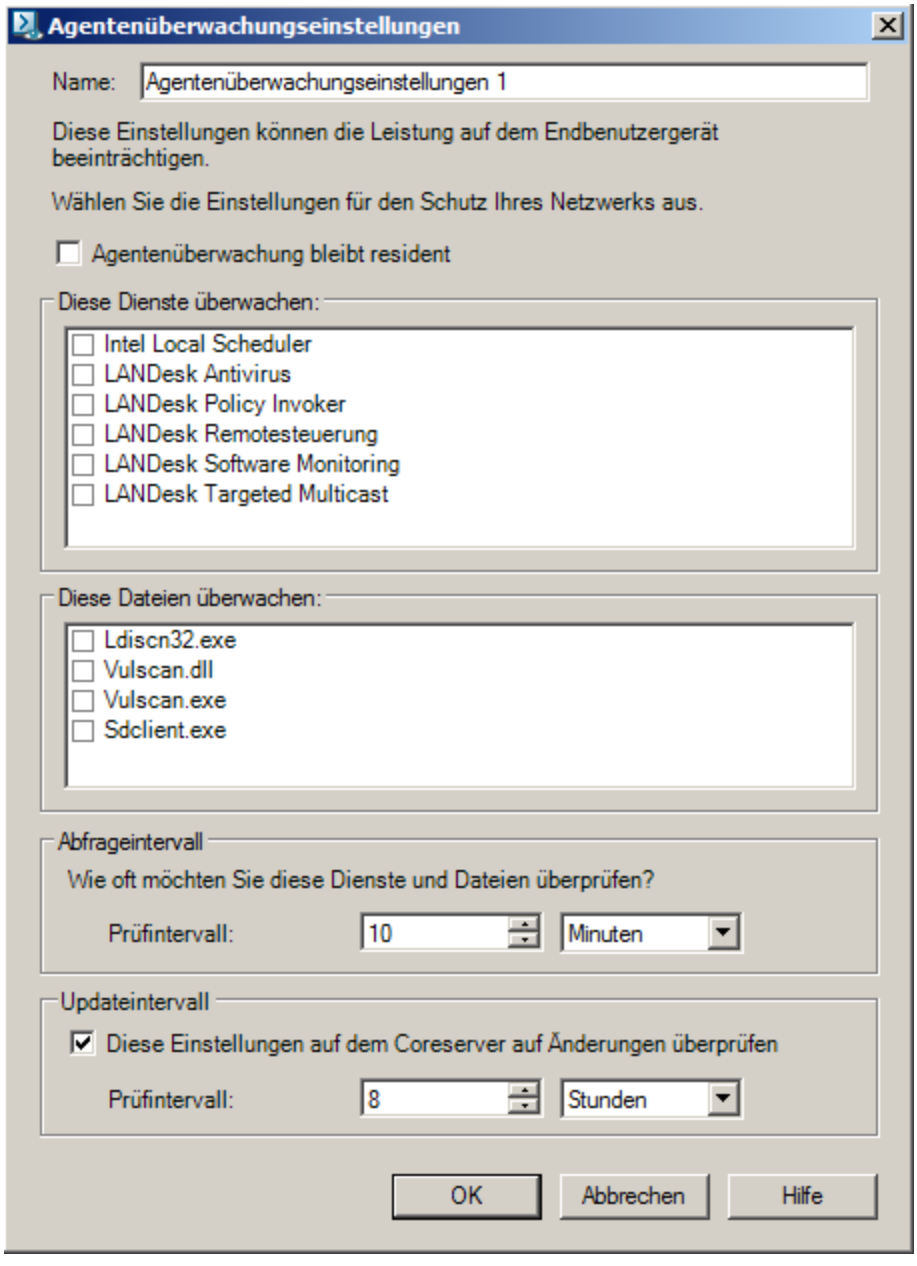
So aktivieren Sie die Agentenüberwachung (oder aktualisieren Sie Einstellungen) mit einem separaten Task

1. Klicken Sie in der Konsole mit der rechten Maustaste auf mindestens ein Gerät und klicken Sie dann auf **Agentenüberwachungseinstellungen aktualisieren**.
2. Aktivieren Sie das Kontrollkästchen **Agentenüberwachung benutzen**.
3. Wählen Sie eine der Einstellungen aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können neue Einstellungen definieren oder vorhandene Einstellungen bearbeiten. Die angewendeten Einstellungen bestimmen, welche Dienste und Dateien wie oft überwacht werden und ob die ausführbare Agentenüberwachungsdatei resident in den Speicher überwachter Geräte geladen wird.
4. Klicken Sie auf **OK**.

Sobald Sie auf die Schaltfläche **OK** klicken, werden alle ausgewählten Zielgeräte mit den neuen Einstellungen aktualisiert und eine entsprechende Statusmeldung eingeblendet.

Konfigurieren der Agentenüberwachungseinstellungen

Mithilfe der Agentenüberwachungseinstellungen (**Extras > Konfiguration > Agentenkonfiguration > Neue Windows Agentenkonfiguration > Sicherheit und Compliance > Agentenüberwachung**) legen Sie fest, welche Dienste und Dateien überwacht werden, wie oft der Status von Diensten und Dateien überprüft werden soll, ob die Agentenüberwachung resident in den Speicher des Geräts geladen wird und ob die zugewiesenen Einstellungen ebenfalls auf Änderungen überprüft werden sollen.



Deaktivieren der Agentenüberwachung auf Geräten

Sie können die Agentenüberwachung auch für ein oder mehrere Geräte deaktivieren (mit dem Task "Agentenüberwachungseinstellungen aktualisieren").

So deaktivieren Sie die Agentenüberwachung

1. Klicken Sie in der Konsole mit der rechten Maustaste auf mindestens ein Gerät und klicken Sie dann auf **Agentenüberwachungseinstellungen aktualisieren**.
2. Stellen Sie sicher, dass das Kontrollkästchen **Agentenüberwachung verwenden** deaktiviert ist.
3. Klicken Sie auf **OK**.

Generieren von Agentenüberwachungsberichten

Die Überwachungs- und Alarminformationen der Agentenüberwachung werden in mehreren Berichten im Extra "Berichte" dargestellt.

Alle Agentenüberwachungsberichte enthalten den Hostnamen der Arbeitsstation, den überwachten Dienst bzw. die überwachte Datei, den Alarmstatus (entweder "gefunden" oder "gelöst") und das Datum, an dem das Ereignis erkannt wurde.

Die Agentenüberwachung speichert den Alarmstatus, sodass der Core beim Entdecken der Bedingung und nach ihrer Beseitigung nur jeweils einen Alarm enthält. Mehrere Alarme können ausgelöst werden, wenn die Agentenüberwachung neu gestartet wird, um das System neu zu booten, oder wenn eine neue Konfiguration mittels Push- oder Pull-Prozedur auf der Arbeitsstation bereitgestellt wird.

Berichte können darüber hinaus auch für eine bestimmte Kategorie auf der Basis unterschiedlicher Intervalle bereitgestellt werden, wie zum Beispiel "Heute", "Letzte Woche", "Letzte 30 Tage" oder ein anderes festgelegtes Intervall.

WICHTIG: Alarmdaten der Agentenüberwachung werden automatisch nach 90 Tagen entfernt
Alle Agentenüberwachungs-Alarmdaten, die älter als 90 Tage sind, werden automatisch aus der Datenbank entfernt. Alarmdaten werden zum Generieren von Agentenüberwachungsberichten verwendet.

WICHTIG: Erforderliche Rechte und Rollen für die Verwendung des Extras "Berichte"
Um auf das Extra "Berichte" zugreifen und Berichte generieren und anzeigen zu können, müssen Benutzer über das Recht "LANDesk Administrator" (d. h. uneingeschränkte Rechte) und die spezifischen Rollen für "Berichte" verfügen.

Weitere Informationen zur Verwendung des Extras "Berichte" finden Sie unter "Berichte" auf Seite 209.

Agentenüberwachungsberichte

Die verfügbaren Agentenüberwachungsberichte sind nachstehend aufgeführt:

Diensttypen konnten nicht geändert werden

In diesem Bericht werden alle Agentenüberwachungsalarme von Arbeitsstationen aufgelistet, denen es nicht gelungen ist, den Starttyp eines überwachten Dienstes zu ändern.

Benötigte Dienste wurden nicht installiert

In diesem Bericht werden alle Agentenüberwachungsalarme von Arbeitsstationen aufgelistet, auf denen ein überwachter Dienst deinstalliert wurde.

Benötigte Dienste wurden nicht gestartet

In diesem Bericht werden alle Agentenüberwachungsalarme von Arbeitsstationen aufgelistet, auf denen ein überwachter Dienst von der Agentenüberwachung nicht neu gestartet werden kann.

Dateien, die nicht auf Clients gefunden wurden

In diesem Bericht werden alle Agentenüberwachungsalarme von Arbeitsstationen aufgelistet, auf denen überwachte Agentendateien gelöscht wurden.

Zum Löschen vorgesehene Dateien auf Clients gefunden

In diesem Bericht werden alle Agentenüberwachungsalarme von Arbeitsstationen aufgelistet, auf denen die überwachten Agentendateien beim Neustart zu löschen sind. Die Agentenüberwachung entfernt diese Dateien auch automatisch aus der Windows-Registrierung.

Hilfe zur Agentenüberwachung

Dieses Kapitel enthält die folgenden Hilfethemen, in denen die Dialogfelder der Agentenüberwachung beschrieben werden.

Informationen zum Dialogfeld "Agentenüberwachungseinstellungen konfigurieren"

Dieses Dialogfeld verwenden Sie zur Verwaltung Ihrer Einstellungen. Nachdem Sie die Einstellungen konfiguriert haben, können Sie diese über eine Agentenkonfiguration oder mithilfe eines Tasks zum Ändern von Einstellungen auf verwaltete Geräte übertragen.

Die Agentenüberwachung ermöglicht es Ihnen, mehrere unterschiedliche Einstellungen zu erstellen, die Geräten und Gerätegruppen zugewiesen werden können.

Dieses Dialogfeld enthält folgende Optionen:

- **Neu:** Öffnet das Dialogfeld "Einstellungen", in dem Sie die Optionen konfigurieren können.
- **Bearbeiten:** Öffnet das Dialogfeld "Einstellungen". In diesem Dialogfeld können Sie die ausgewählten Einstellungen bearbeiten.
- **Kopieren:** Öffnet eine Kopie der ausgewählten Einstellungen als Vorlage, die von Ihnen dann bearbeitet und umbenannt werden können.
- **Löschen:** Entfernt die ausgewählten Einstellungen aus der Datenbank.
- **Schließen:** Schließt das Dialogfeld, ohne Einstellungen auf den Task anzuwenden.

Informationen zum Dialogfeld "Agentenüberwachungseinstellungen"

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten von Agentenüberwachungseinstellungen.

Agentenüberwachungseinstellungen bestimmen, welche Dienste und Dateien wie oft überwacht werden und ob das Dienstprogramm auf dem Gerät verbleibt.

Dieses Dialogfeld enthält folgende Optionen:

- **Name:** Kennzeichnet die Einstellungen mit einem eindeutigen Namen.
- **Agentenüberwachung bleibt resident:** Gibt an, ob die LDRegwatch.exe (Agentenüberwachungs-Programmdatei) dauerhaft im Speicher resident bleibt. Wenn Sie diese Option nicht aktivieren, bleibt LDRegwatch.exe nur so lange im Speicher, wie in Übereinstimmung mit dem Zeitplan zum Überprüfen der ausgewählten Dienste und Dateien erforderlich.
- **Diese Dienste überwachen:** Gibt an, welche kritischen Dienste mit diesen Agentenüberwachungseinstellungen überwacht werden.
- **Diese Dateien überwachen:** Gibt an, welche kritischen Dateien mit diesen Agentenüberwachungseinstellungen überwacht werden.
- **Abfrageintervall:** Gibt an, wie oft die Agentenüberwachung die ausgewählten Dienste und Dateien überwachen soll. Der Mindestwert für dieses Intervall beträgt 30 Sekunden.
- **Diese Einstellungen auf dem Coreserver auf Änderungen überprüfen:** Vergleicht automatisch die aktuelle Version der ausgewählten Agentenüberwachungseinstellungen mit der auf den Zielgeräten bereitgestellten Version (im angegebenen Intervall). Wenn festgestellt wird, dass die Einstellungen innerhalb der angegebenen Zeitspanne geändert wurden, werden die neuen Einstellungen bereitgestellt und die Agentenüberwachung wird mit den neuen Einstellungen neu gestartet.
    - **Prüfintervall:** Gibt die Zeitspanne für die wiederkehrenden Vergleiche der Agentenüberwachungseinstellungen an.

WICHTIG: Nicht von Ihnen bereitgestellte Dienste sollten nicht für die Überwachung durch die Agentenüberwachung ausgewählt werden
Wählen Sie beim Konfigurieren von Agentenüberwachungseinstellungen keine Dienste aus, die von Ihnen nicht für die Installation auf Zielgeräten vorgesehen sind. Andernfalls erhält der Coreserver Alarmmeldungen für nicht installierte Dienste, die absichtlich nicht installiert wurden. Beachten Sie jedoch, dass selbst wenn ein nicht installierter Dienst für die Überwachung ausgewählt wird, keine Alarmmeldungen (die sich darauf beziehen, dass der Dienst sich nicht neu starten oder sein Starttyp sich nicht ändern lässt) gesendet werden.

Informationen zum Dialogfeld "Agentenüberwachungseinstellungen aktualisieren"

Dieses Dialogfeld verwenden Sie zur Aktualisierung der Agentenüberwachungseinstellungen auf Zielgeräten und zur Aktivierung oder Deaktivierung des Dienstprogramms "Agentenüberwachung" auf Zielgeräten.

Wenn die Agentenüberwachung auf den ausgewählten Arbeitsstationen nicht aktiv ist, aktivieren Sie das Kontrollkästchen **Agentenüberwachung benutzen**, konfigurieren die Agentenüberwachungseinstellungen und klicken dann auf **OK**. Die Agentenüberwachung wird aktiviert, nachdem die Konfiguration auf die ausgewählten Geräte übertragen wurde (mittels "Push"-Prozedur). Um die überwachten Dateien oder Dienste zu ändern, klicken Sie auf die Schaltfläche **Konfigurieren**, um das Dialogfeld **Agentenüberwachungseinstellungen** zu öffnen.

Sie können die Agentenüberwachung mithilfe des Dialogfeldes "Agentenüberwachungseinstellungen aktualisieren" auch deaktivieren, indem Sie die Aktivierung des Kontrollkästchens **Agentenüberwachung benutzen** aufheben und auf **OK** klicken.

Dieses Dialogfeld enthält folgende Optionen:

- **Agentenüberwachung benutzen:** Aktiviert den Agentenüberwachungsdienst auf Zielgeräten.
- **Agentenüberwachungseinstellung auswählen:** Gibt an, welche Einstellung für den Task verwendet wird. Wählen Sie eine der Einstellungen aus der Liste aus oder klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen.

Sobald die Schaltfläche **OK** ausgewählt ist, werden alle ausgewählten Geräte mit den neuen Einstellungen aktualisiert und eine entsprechende Statusmeldung eingeblendet.

Inventar

Übersicht über das Inventarscannen

Der Inventarscanner erfasst Hardware- und Softwaredaten und fügt sie in die Coredatenbank ein. Wenn Sie ein Gerät mit dem Tool "Agentenkonfiguration" konfigurieren, gehört der Inventarscanner zu den Komponenten des Standard Management Suite Agent, die auf dem Gerät installiert werden. Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Ein Gerät gilt als verwaltet, sobald es einen Inventarscan an die Coredatenbank sendet. Die Windows-Scanner-Programmdatei trägt den Namen ldiscn32.exe.

Es gibt zwei verschiedene Inventarscans:

- **Hardwarescan**: Scannt Hardwaredaten auf verwalteten Geräten. Hardwarescans werden schnell ausgeführt. Sie können das Intervall für den Hardwarescan in einer Agentenkonfiguration (**Extras > Konfiguration > Agentenkonfiguration**) festlegen und auf verwalteten Geräten bereitstellen. Standardmäßig werden Hardwarescans bei jedem Gerätestart ausgeführt.
- **Softwarescan**: Scannt installierte Software auf verwalteten Geräten. Diese Scans benötigen mehr Zeit für die Ausführung als Hardwarescans. Softwarescans können mehrere Minuten beanspruchen, je nachdem, wie viele Dateien sich auf dem verwalteten Gerät befinden. Standardmäßig wird der Softwarescan nur einmal am Tag ausgeführt, ganz gleich, wie oft der Inventarscanner auf dem Gerät ausgeführt wird. Sie können das Intervall für den Softwarescan auf der Registerkarte **Konfigurieren > Dienste konfigurieren > Inventar** konfigurieren.

Sie können ein Gerät individuell scannen, indem Sie es in der Netzwerkansicht ausfindig machen, mit der rechten Maustaste darauf klicken und dann **Inventarscan** wählen.

HINWEIS: Ein Gerät, das über die Erkennungsfunktion zur Coredatenbank hinzugefügt wurde, hat seine Inventardaten noch nicht in die Coredatenbank gescannt. Sie müssen einen Inventarscan auf jedem Gerät ausführen, damit die gesamten Inventardaten für dieses Gerät angezeigt werden.

Sie können Inventardaten anzeigen lassen und wie folgt verwenden:

- Die Spalten der Netzwerkansicht anpassen, um bestimmte Inventarattribute anzuzeigen
- Die Coredatenbank nach Geräten mit bestimmten Inventarattributen durchsuchen
- Geräte gruppieren, um Verwaltungstasks wie die Softwareverteilung zu beschleunigen
- Spezielle Berichte basierend auf Inventarattributen generieren

Mithilfe der Inventarscans können Sie auch Hardware- und Softwareänderungen auf Geräten verfolgen und beim Auftreten solcher Ereignisse Warnungen generieren und Einträge in die Protokolldatei schreiben lassen. Weitere Informationen finden Sie unter "Verfolgen von Inventaränderungen" auf Seite 160.

Optimierung des Inventarscans

Nachstehend werden einige Optionen beschrieben, die Ihnen zur Optimierung von Inventarscans zur Verfügung stehen.

Deltascannen

Nach dem ersten vollständigen Scan auf einem Gerät erfasst der Inventarscanner nur Deltaänderungen und sendet diese an die Coredatenbank. Indem nur geänderte Daten gesendet werden, werden Netzwerkverkehr und Datenverarbeitungszeit minimiert.

Erzwingen eines vollständigen Scans

Wenn Sie einen vollständigen Scan der Hardware- und Softwaredaten des Geräts erzwingen möchten, können Sie die vorhandene Deltascandatei löschen und die entsprechende Einstellung im Applet LANDesk Softwaredienste konfigurieren (**Konfigurieren > Dienste**) ändern.

1. Löschen Sie die Datei **invdelta.dat** vom Gerät. Eine Kopie des letzten Inventarscans ist lokal als verborgene Datei mit dem Namen "invdelta.dat" gespeichert. Die Umgebungsvariable LDMS_LOCAL_DIR legt den Pfad dieser Datei fest. Standardmäßig ist dies das Verzeichnis C:\Programme\LANDesk\LDClient\Data.
2. Fügen Sie die Option **/sync** in die Befehlszeile des Inventarscanners ein. Um die Befehlszeile zu bearbeiten, klicken Sie auf **Start > Alle Programme > LANDesk Management**, klicken mit der rechten Maustaste auf das Shortcutsymbol **Inventarscan**, wählen **Eigenschaften > Shortcut** aus und bearbeiten dann den **Zielpfad**.
3. Klicken Sie beim Coreserver auf **Start > Alle Programme > LANDesk > LANDesk Dienste konfigurieren**.
4. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
5. Klicken Sie auf die Einstellung **Do Delta**. Geben Sie in das **Wert**-Feld **0** ein.
6. Klicken Sie zweimal auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Scankomprimierung

Inventarscans mit dem Windows-Inventarscanner (ldiscn32.exe) werden standardmäßig komprimiert. Der Scanner komprimiert vollständige und Deltascans in einem Komprimierungsverhältnis von ca. 8:1. Scans werden zunächst vollständig im Speicher erstellt, dann komprimiert und mithilfe eines größeren Pakets an den Coreserver gesendet. Die Scankomprimierung reduziert die Anzahl der erforderlichen Pakete und die Bandbreitennutzung.

Scanverschlüsselung

Inventarscans sind standardmäßig verschlüsselt (nur TCP/IP-Scans). Sie können die Inventarscan-Verschlüsselung deaktivieren, indem Sie die entsprechende Einstellung im Applet LANDesk Softwaredienste konfigurieren (**Konfigurieren > Dienste**) ändern.

1. Klicken Sie beim Coreserver auf **Start > Alle Programme > LANDesk > LANDesk Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
3. Klicken Sie auf die Einstellung **Verschlüsselung deaktivieren**. Geben Sie in das **Wert**-Feld **1** ein.
4. Klicken Sie auf **Festlegen** und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Verschlüsselter Datentransport.

Es gibt auf der Registerkarte **Konfigurieren > Dienste > Inventar** eine Option mit der Bezeichnung **Verschlüsselter Datentransport**. Diese Option veranlasst, dass Gerätescans unter Verwendung von SSL an den Core gesendet werden. Da die Dateien über den Webdienst und nicht das Frontend des Inventardienstes gesendet werden, wird keine NAT-Adresse an die Scandatei angefügt - sogar dann nicht, wenn diese Option in der Registrierung aktiviert ist.

Anzeigen von Inventardaten

Sobald ein Gerät vom Inventarscanner geprüft wurde, können Sie dessen Systeminformationen in der Konsole anzeigen.

Geräteinventardaten werden in der Coredatenbank gespeichert. Sie umfassen Hardware-, Gerätetreiber-, Software-, Speicher- und Umgebungsinformationen. Die Inventardaten sind beim Verwalten und Konfigurieren von Geräten hilfreich. Außerdem können Sie damit schnell Systemprobleme erkennen.

Sie können Inventardaten entweder in Form einer Übersicht oder als vollständiges Geräteinventar anzeigen. Darüber hinaus können Inventardaten auch in von Ihnen generierten Berichten angezeigt werden. Weitere Informationen hierzu finden Sie unter "Berichte" auf Seite 209.

Anzeigen einer Inventarübersicht

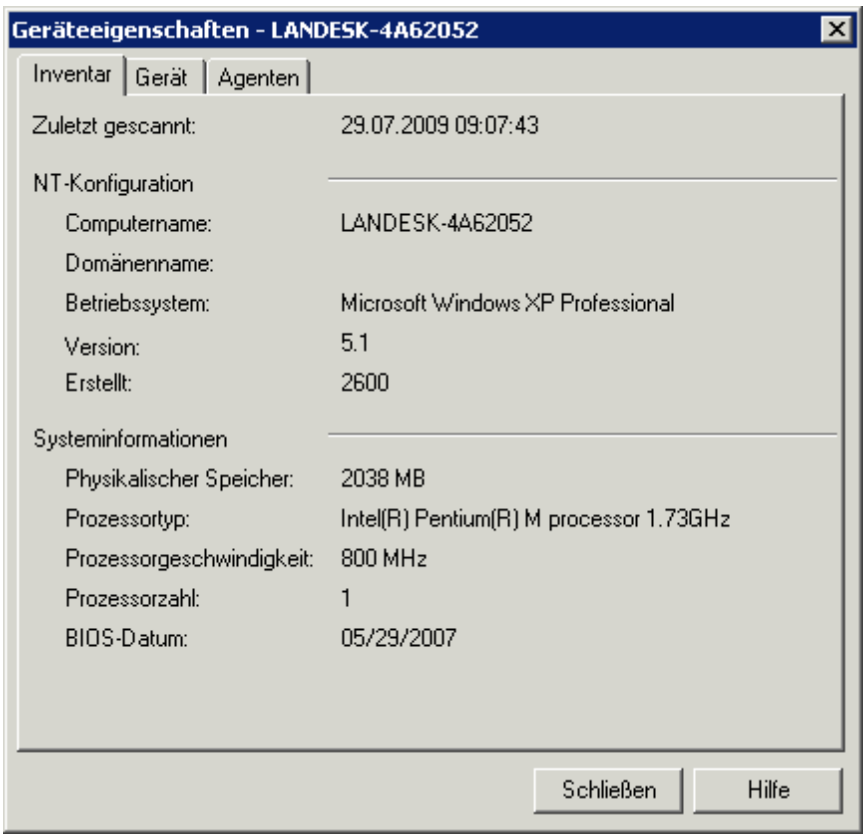
Eine Inventarübersicht finden Sie auf der Eigenschaftsseite des Geräts. Sie bietet eine schnelle Übersicht über die Betriebssystemkonfiguration sowie Systeminformationen des Geräts. Die Übersicht zeigt außerdem Datum und Uhrzeit des letzten Inventarscans, damit Sie wissen, wie aktuell die Daten sind.

HINWEIS: Wenn Sie ein Gerät mithilfe des Erkennungstool in die Coredatenbank eingefügt haben, sind seine Inventardaten noch nicht in die Coredatenbank gescannt. Sie müssen einen Inventarscan auf dem Gerät ausführen, damit die zugehörigen Inventardaten angezeigt werden.

So zeigen Sie eine Inventarübersicht an

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf ein Gerät.
2. Klicken Sie auf **Eigenschaften** > Registerkarte **Inventar**.

Bild anzeigen/ausblenden



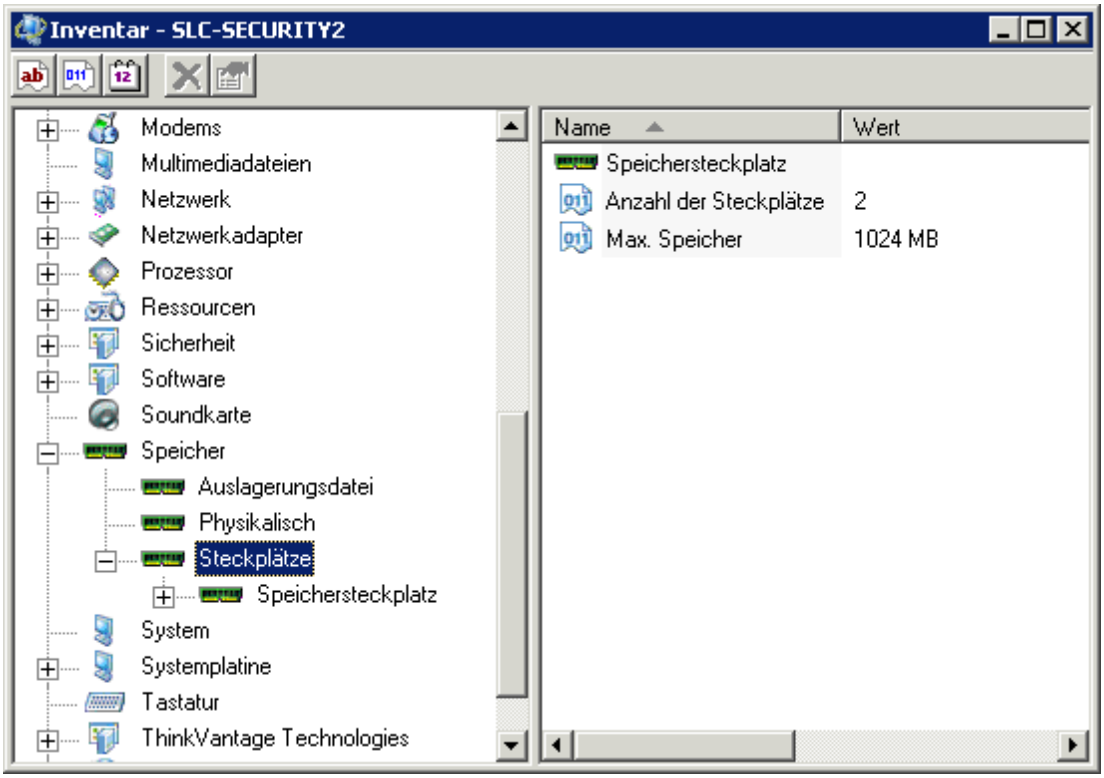
Anzeigen eines vollständigen Inventars

Ein vollständiges Inventar umfasst eine komplette und ausführliche Aufstellung der Hardware- und Softwarekomponenten eines Geräts. Die Aufstellung enthält Objekte und Objektattribute.

So zeigen Sie ein vollständiges Inventar an

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf ein **Gerät**.
2. Klicken Sie auf **Inventar**.

Bild anzeigen/ausblenden



Genauere Informationen finden Sie unter "Hilfe zum Inventar" auf Seite 188.

Anzeigen von Attributeigenschaften

In der Inventarliste können Sie Attributeigenschaften für die Inventarobjekte eines Geräts anzeigen. Attributeigenschaften geben Aufschluss über die Eigenschaften und Werte eines Inventarobjekts. Sie können auch neue, angepasste Attribute erstellen und benutzerdefinierte Attribute bearbeiten.

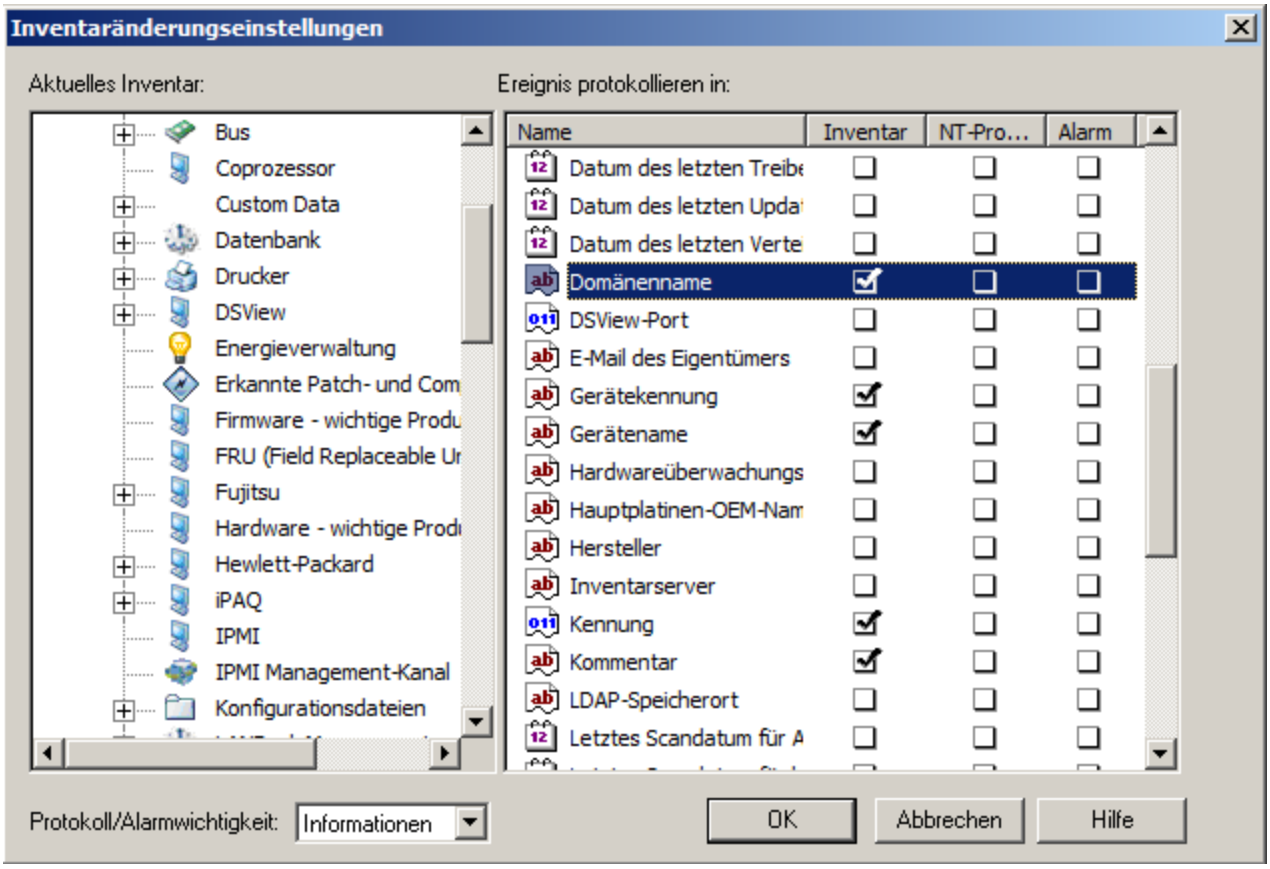
Um die Eigenschaften eines Attributs anzuzeigen, doppelklicken Sie auf das Attribut.

Nähere Informationen finden Sie unter "Informationen zum Dialogfeld "Eigenschaften des Inventarattributs"" auf Seite 190.

Verfolgen von Inventaränderungen

LANDesk kann Änderungen an der Hardware und Software des Geräts erkennen und aufzeichnen. Wenn Sie Inventaränderungen verfolgen, haben Sie einen besseren Überblick über Ihren Netzwerkbestand. Mit den Inventaränderungseinstellungen können Sie auswählen, welche Arten von Änderungen mit welcher Priorität gespeichert werden sollen. Die ausgewählten Änderungen können in einem Inventarverlaufsprotokoll oder dem Windows-Ereignisprotokoll des Coreservers gespeichert oder als AMS-Alarm gesendet werden.

Bild anzeigen/ausblenden



Sie können den Verlauf der Inventaränderungen eines Geräts anzeigen und drucken. Zusätzlich können Sie Inventaränderungen in eine CSV-formatierte Datei für Analysen mit eigenen Berichterstellungstools exportieren.

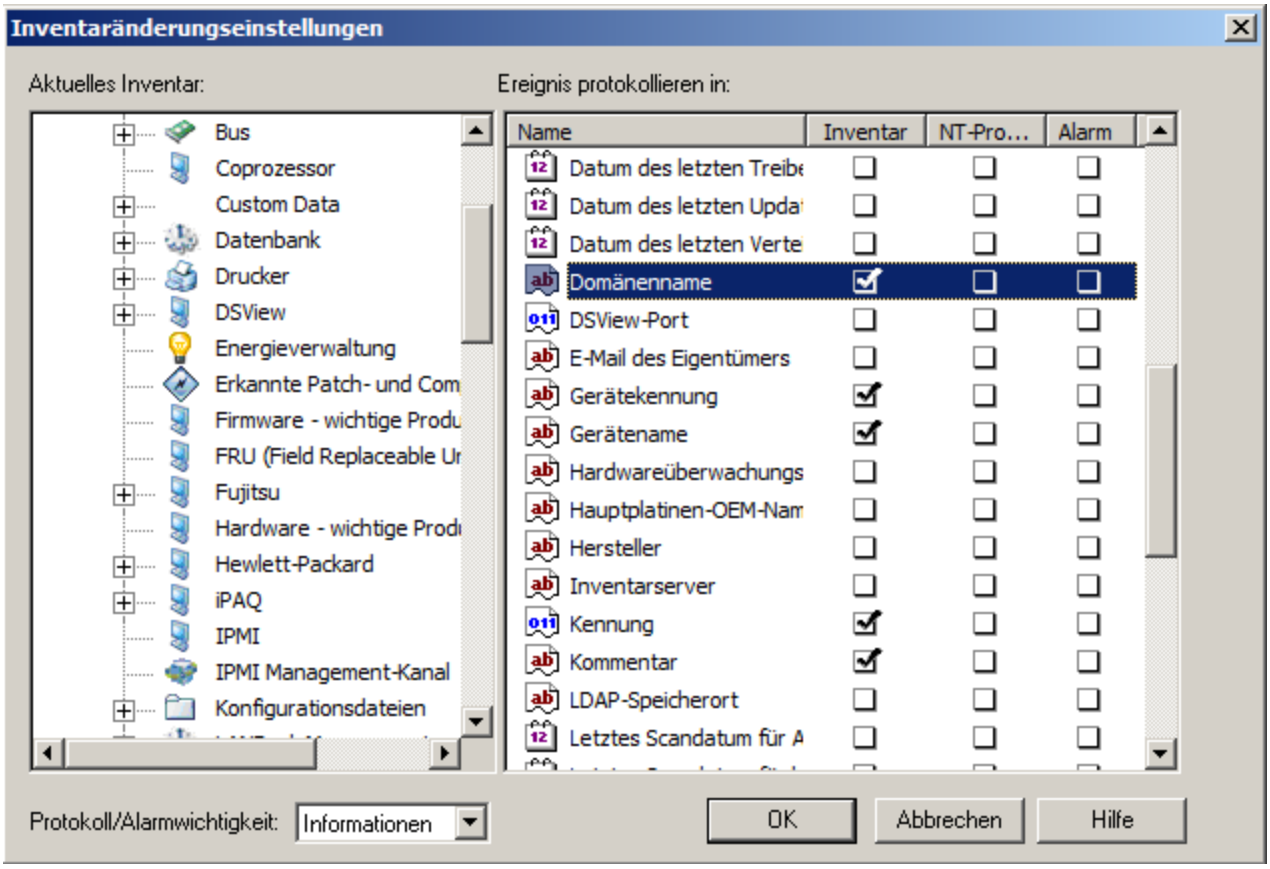
Um Inventaränderungen zu verfolgen und zu nutzen, müssen Sie zuerst die Inventaränderungseinstellungen konfigurieren. Sie können die anderen Tasks in Bezug auf den Inventaränderungsverlauf ausführen:

- "Konfigurieren von Inventaränderungseinstellungen" auf Seite 161
- "Anzeigen, Drucken und Exportieren von Inventaränderungen" auf Seite 162

Konfigurieren von Inventaränderungseinstellungen

HINWEIS: Sie müssen zuerst diese Einstellungen konfigurieren, wenn Sie Inventaränderungen für ein Gerät im Netzwerk anzeigen, drucken oder exportieren möchten.

Bild anzeigen/ausblenden



So konfigurieren Sie Inventaränderungseinstellungen

1. Klicken Sie auf **Konfigurieren** > **Inventarverlauf**.
2. Erweitern Sie im Dialogfeld **Inventaränderungseinstellungen** in der Liste **Aktuelles Inventar** das Objekt **Computer** und wählen Sie anschließend die zu verfolgenden Systemkomponenten aus.
3. Wählen Sie in der Liste **Ereignis protokollieren in** das Attribut der Komponente aus, das verfolgt werden soll.
4. Aktivieren Sie das entsprechende Kontrollkästchen, um anzugeben, wo Änderungen dieses Attributs erfasst werden sollen. Inventaränderungen können im Protokoll des Inventaränderungsverlaufs, im Protokoll der Windows NT-Ereignisanzeige oder als AMS-Alarm aufgezeichnet werden.
5. Wählen Sie eine Priorität in der Dropdownliste **Protokoll/Alarmwichtigkeit** aus. Folgende Prioritätsstufen können ausgewählt werden: Keine, Informationen, Warnung und Kritisch.
6. Klicken Sie auf **OK.**

Nähere Informationen finden Sie unter "Informationen zum Dialogfeld "Inventaränderungseinstellungen"" auf Seite 190.

Anzeigen, Drucken und Exportieren von Inventaränderungen

So öffnen, drucken oder exportieren Sie Inventaränderungen

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf ein Gerät.
2. Klicken Sie auf **Inventarverlauf**.

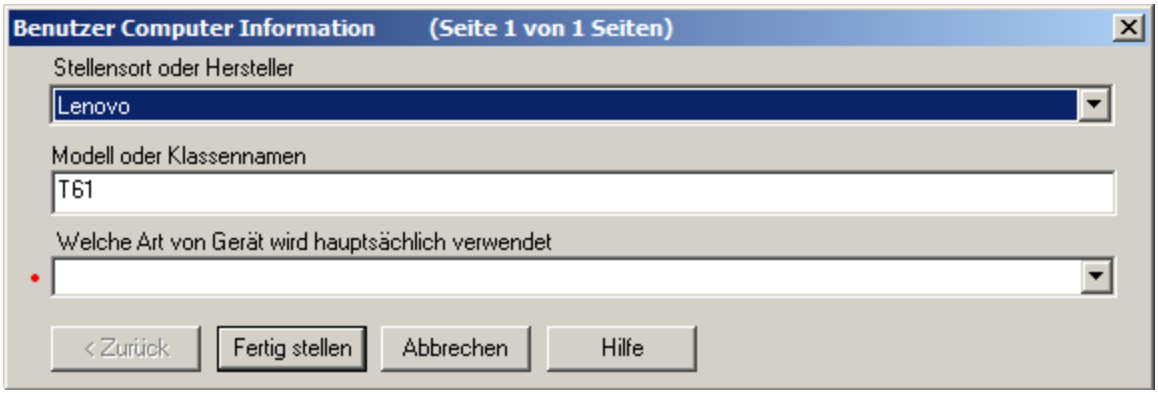
3. Klicken Sie auf **Drucken**, um den Inventaränderungsverlauf zu drucken.
4. Klicken Sie auf **Exportieren**, um den Inventaränderungsverlauf als CSV-Datei zu speichern.

Nähere Informationen finden Sie unter "Informationen zum Dialogfeld "Inventaränderungsverlauf"" auf Seite 190.

Verwenden von benutzerdefinierten Datenformularen

LANDesk enthält ein Extra für benutzerdefinierte Datenformulare (**Extras** > **Konfiguration** > **Benutzerdefinierte Datenformulare**), mit dem Sie Formulare erstellen und verwalten können. Mithilfe von benutzerdefinierten Datenformularen können Sie Informationen von Benutzern erfassen und in die Coredatenbank einfügen.

Bild anzeigen/ausblenden



HINWEIS: Benutzerdefinierte Datenformulare werden in LANDesk Security Suitenicht unterstützt. Benutzerdefinierte Datenformulare stehen bei einer reinen LANDesk Security Suite Lizenz nicht zur Verfügung. Sie müssen im Besitz einer LANDesk Management Suite Volllizenz sein, um die Funktion "Benutzerdefinierte Formulare" verwenden zu können.

Bestimmte benutzerspezifische Informationen können vom Inventarscanner nicht erfasst werden. Beispiele:

- der Standort des Schreibtischs eines Benutzers,
- die Assetnummer eines Computers,
- die Telefonnummer eines Benutzers.

Diese Angaben erfassen Sie am besten mit benutzerdefinierten Datenformularen direkt von den Benutzern.

Benutzerdefinierte Datenformulare bestehen aus zwei Hauptkomponenten: dem Formular-Designer, mit dem Sie vom Benutzer auszufüllende Formulare erstellen, und der Formularanzeige, mit dem Benutzer Formulare ausfüllen.

Formulare können zentral oder lokal gespeichert werden. Wenn sie zentral gespeichert werden, haben alle Benutzer automatisch Zugriff auf die neuesten Formulare, weil jeder dasselbe Formular am selben Speicherplatz sieht. Wenn Formulare lokal gespeichert werden, müssen Sie sicherstellen, dass Benutzer die neuesten Formulare erhalten.

Nachdem ein Benutzer ein Formular ausgefüllt hat, speichert die Formularanzeige die Ergebnisse lokal in C:\Programme\LANDesk\LDClient\ldcstm.dat. Diese Datei enthält die Ergebnisse aller Formulare, die der Benutzer ausgefüllt hat. Diese Datei enthält die Ergebnisse aller Formulare, die ein Benutzer ausgefüllt hat. Wenn der Benutzer dasselbe Formular noch einmal ausfüllen muss (z. B. wenn das Originalformular überarbeitet wurde), fügt die Formularanzeige automatisch die zuvor eingegebenen Daten ein.

Der Inventarscanner nimmt die Informationen aus der Datei ldcstm.dat eines jeden Geräts und fügt sie zur Coredatenbank hinzu.

HINWEIS: Bei Oracle-Datenbanken muss die Groß-/Kleinschreibung beachtet werden.
Wenn Sie in einer Oracle-Datenbank benutzerdefinierte Felder mit benutzerdefinierten Datenformularen erstellen (oder eine beliebige andere Funktion verwenden), müssen Sie bei den Feldnamen auf Groß-/Kleinschreibung achten. Beispiel: Mit "Standort" verknüpfte Daten werden in einem anderen Speicherort der Datenbank gespeichert als Daten, die mit "STANDORT verknüpft sind.

Stellen Sie außerdem sicher, dass benutzerdefinierte Felder unabhängig von der Großschreibung eindeutige Namen besitzen. Unter Umständen werden die falschen Inventardaten abgerufen, wenn zwei benutzerdefinierte Felder denselben Namen mit unterschiedlicher Groß-/Kleinschreibung verwenden.

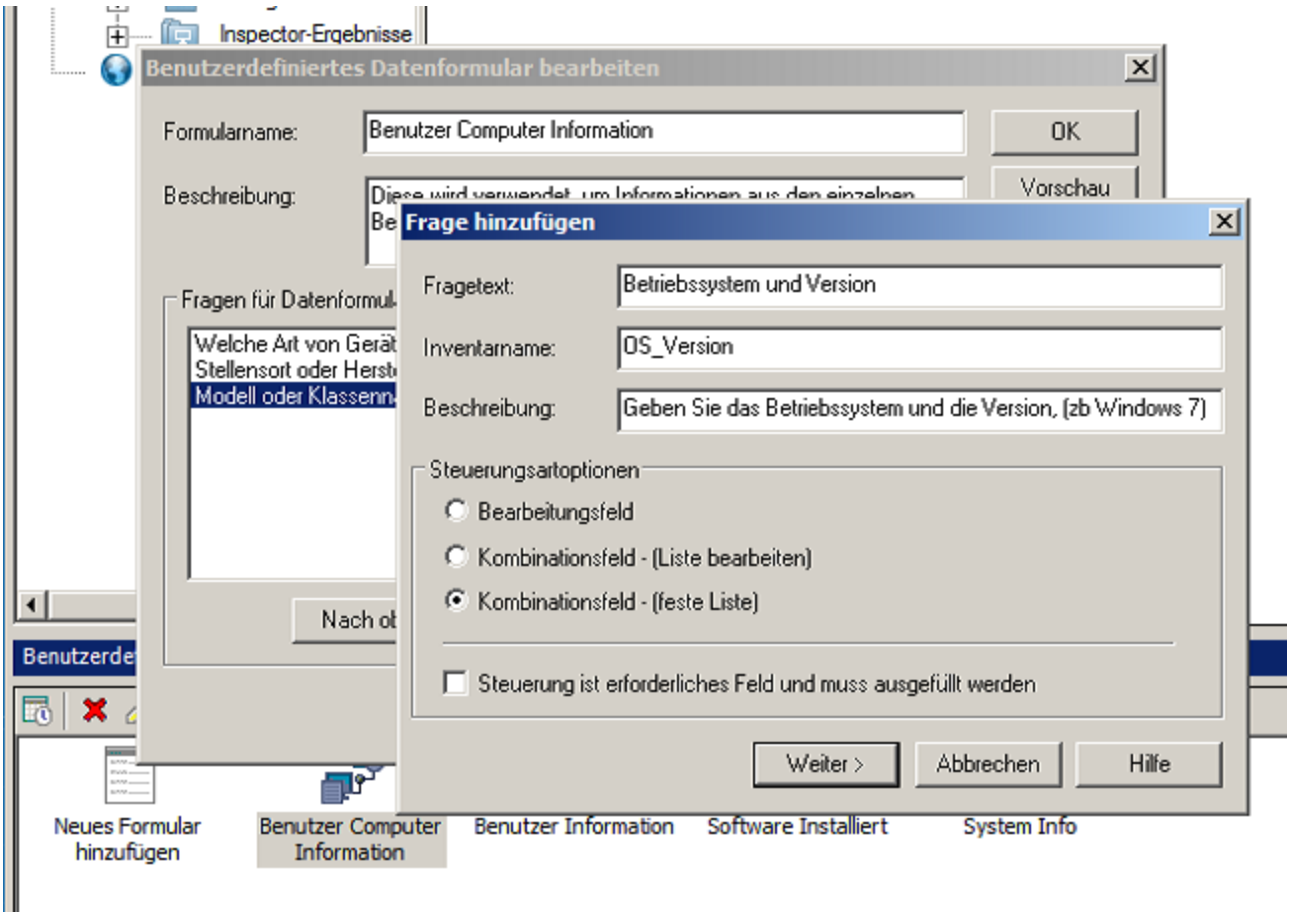
Erstellen eines benutzerdefinierten Datenformulars

Mithilfe von benutzerdefinierten Datenformularen können Sie Informationen von Benutzern erfassen und in die Coredatenbank einfügen. Führen Sie folgende Schritte aus, um ein benutzerdefiniertes Datenformular zu erstellen.

So erstellen Sie ein benutzerdefiniertes Datenformular

1. Klicken Sie auf **Extras > Konfiguration > Benutzerdefinierte Datenformulare**.
2. Doppelklicken Sie im Fenster "Benutzerdefinierte Datenformulare" auf **Neues Formular hinzufügen**.
3. Geben Sie einen Namen für das Formular ein.
4. Geben Sie eine Beschreibung für das Formular ein. (Die von Ihnen eingegebene Beschreibung wird als Hilfetipp angezeigt, wenn der Benutzer beim Ausfüllen des Formulars in dem Feld auf F1 klickt.)
5. Klicken Sie auf **Hinzufügen**, um das Dialogfeld **Frage hinzufügen** zu öffnen.
6. Geben Sie im Dialogfeld "Frage hinzufügen" Informationen in die Felder **Fragetext**, **Inventarname** und **Beschreibung** ein.
7. Wählen Sie die **Steuerungsart** aus.
8. Geben Sie an, ob das Feld ein erforderliches Feld sein soll.
9. Wenn Sie die Steuerungsart **Bearbeitungsfeld** auswählen, klicken Sie auf **Beenden**, um das Dialogfeld **Frage hinzufügen** zu schließen. Mit der Steuerungsart "Bearbeitungsfeld" können Benutzer eigene Antworten in ein editierbares Textfeld eingeben. Sie können weitere Fragen hinzufügen oder mit Schritt 12 fortfahren.

Bild anzeigen/ausblenden



10. Wenn Sie eine der Steuerungsarten **Kombinationsfeld** auswählen, klicken Sie auf **Weiter**, um das Dialogfeld **Elemente hinzufügen** zu öffnen. Mit der Steuerungsart "Kombinationsfeld" können Benutzer ihre Antworten in einer Dropdownliste mit vordefinierten Elementen auswählen.
11. Geben Sie im Dialogfeld "Elemente hinzufügen" einen Elementnamen ein und klicken Sie auf **Einfügen**, um das Element in die Elementliste einzufügen. Diese Elemente werden in einer Dropdownliste für diese Frage auf dem Formular angezeigt. Sie können beliebig viele Elemente hinzufügen, bevor Sie auf **Beenden** klicken.
12. Wenn Sie keine weiteren Fragen hinzufügen möchten, klicken Sie auf **Schließen**, um das Formular zu speichern.

Wenn Sie mit der rechten Maustaste auf ein Formular klicken, können Sie seine Verteilung an Geräte planen.

Erstellen einer Gruppe von Formularen

Wenn Sie mehrere Formulare an Geräte verteilen möchten, sollten Sie die Formulare zu einer Gruppe zusammenzufassen. Sie müssen dann lediglich die Verteilung der Formulargruppe planen.

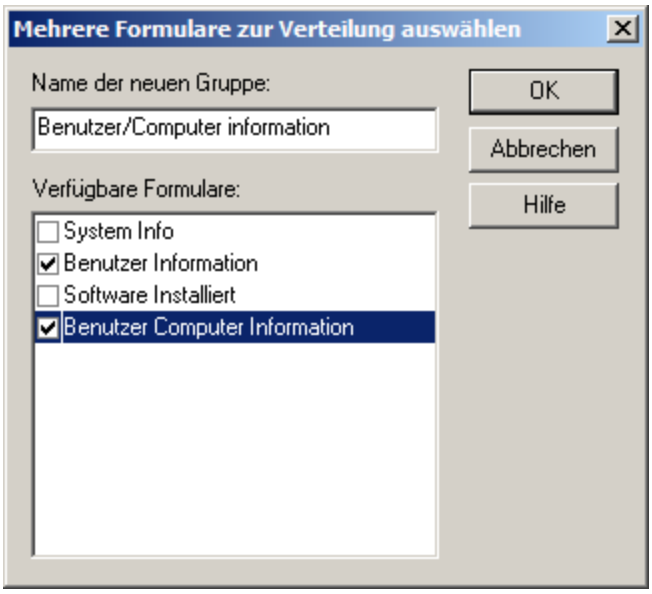
Beim Planen der Verteilung einer Gruppe von Formularen liest der lokale Scheduler den Inhalt der Gruppe zum geplanten Zeitpunkt der Verteilung. Das bedeutet, Sie können den Inhalt der Gruppe auch dann noch ändern, wenn ihre Verteilung bereits geplant ist (solange der geplante Auftrag noch nicht ausgeführt wurde).

HINWEIS: Wenn ein Formular der Gruppe später geändert oder gelöscht wird, spiegelt die Gruppe diese Änderungen sofort wider.

So erstellen Sie eine Formulargruppe

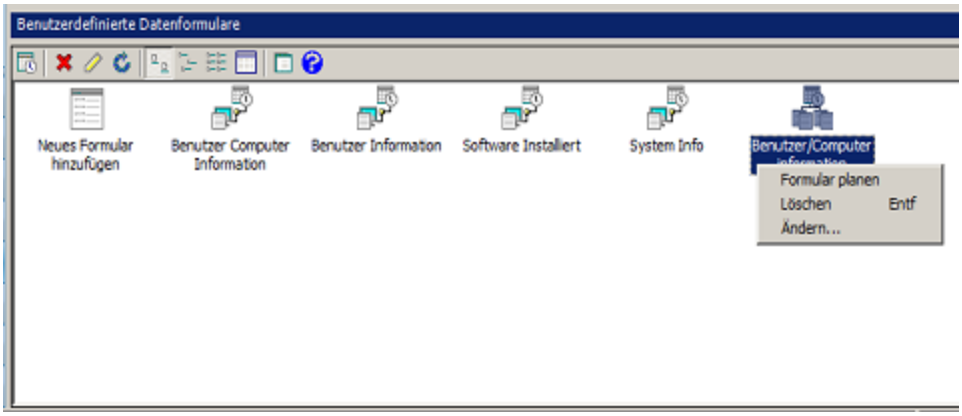
1. Klicken Sie im Fenster **Benutzerdefinierte Datenformulare** auf die Symbolleistenschaltfläche **Mehrere Formulare**.
2. Geben Sie einen Namen für die neue Gruppe ein.
3. Wählen Sie die Formulare, die zur Gruppe hinzugefügt werden sollen, in der Liste der verfügbaren Formulare aus.
4. Klicken Sie auf **OK**.

Bild anzeigen/ausblenden



Sobald Sie eine Gruppe von Formularen erstellt haben, können Sie mit der rechten Maustaste auf eine Gruppe klicken, um sie für die Verteilung an die Geräte einzuplanen.

Bild anzeigen/ausblenden



Konfigurieren von Geräten für den Empfang von benutzerdefinierten Datenformularen

Wenn Sie Geräte einrichten, können Sie festlegen, dass diese Geräte benutzerdefinierte Datenformulare empfangen können. Sie müssen die Komponente "Benutzerdefinierte Datenformulare" installieren und Optionen für benutzerdefinierte Datenformulare im Dialogfeld "Agentenkonfiguration" angeben. Weitere Informationen finden Sie unter "Bereitstellen benutzerdefinierter Datenformulare" auf Seite 125.

Im Dialogfeld "Agentenkonfiguration" müssen Sie festlegen, wie Formulare auf dem Gerät aktualisiert werden:

- **Automatisches Update:** Wenn alle Formulare zentral gespeichert sind (automatische Aktualisierungen), müssen Benutzer nur eine zentrale Stelle nach neuen Formularen durchsuchen. Wenn ein neues Formular zur Verfügung gestellt wird, können alle Geräte, die an dieser Stelle suchen, sofort darauf zugreifen. Der Nachteil ist, dass viele Formulare angezeigt werden, die für den Benutzer nicht relevant sind.
- **Manuelles Update:** Wenn Formulare lokal gespeichert sind (manuelle Aktualisierungen), müssen Sie die Formulare an die Benutzer verteilen, die sie ausfüllen müssen. Dadurch wird das Netzwerk weniger belastet, weil jedes Gerät eine eigene Kopie des Formulars besitzt. Der Vorteil von lokalen Kopien besteht darin, dass Sie die Formulare, die den Benutzern angezeigt werden, auf die für sie relevanten Formulare beschränken können. Formulare können beim Gerätesetup oder mit dem Extra "Geplante Tasks" auf Geräte kopiert werden.

Sie müssen außerdem angeben, wann Formulare auf dem Geräte angezeigt werden:

- **Beim Start:** Die Formularanzeige des Geräts sucht jedes Mal, wenn das Gerät gestartet wird, nach neuen oder geänderten Formularen. Die Formularanzeige wird nach dem Laden des Betriebssystems gestartet. Wenn der Inventarscanner das nächste Mal ausgeführt wird, sendet er ausgefüllte Formulare an die Coredatenbank.
- **Wenn der Inventarscanner ausgeführt wird:** Der Inventarscanner startet die Formularanzeige, die nach neuen oder geänderten Formularen sucht. Sobald Benutzer das Formular komplett ausgefüllt und die Formularanzeige geschlossen haben, wird der Scan beendet und die Daten in die Coredatenbank geschrieben.
- **Beim Starten aus dem LANDesk Programmordner:** Die Formularanzeige kann manuell von der Programmgruppe Management Suite aus gestartet werden. Wenn der Inventarscanner das nächste Mal ausgeführt wird, sendet er ausgefüllte Formulare an die Coredatenbank.

Sie können auch das Fenster **Geplante Tasks** verwenden, um den Formular-Viewer zu einem vorab festgelegten Zeitpunkt auf Geräten zu starten. Verwenden Sie in diesem Szenario das Fenster **Geplante Tasks**, um die Formulare zuerst an Geräte zu verteilen. Räumen Sie genügend Zeit für die Verteilung der Formulare ein, bevor Sie die skriptfähige Aufgabe der Funktion "Geplante Tasks" verwenden, um die Formularanzeige auszuführen.

Ausfüllen von Formularen auf dem Gerät

WICHTIG: Mit dem Extra "Geplante Tasks" (**Verteilung > Geplante Tasks**) können Sie die Bereitstellung benutzerdefinierter Datenformulare (oder Formulargruppen) für Geräten planen. Damit Formulare auf dem Gerät angezeigt werden, müssen Sie außerdem die Anzeige von Formularen im Extra "Agentenkonfiguration" aktivieren (**Konfiguration > Agentenkonfiguration >** (**Doppelklick auf die**

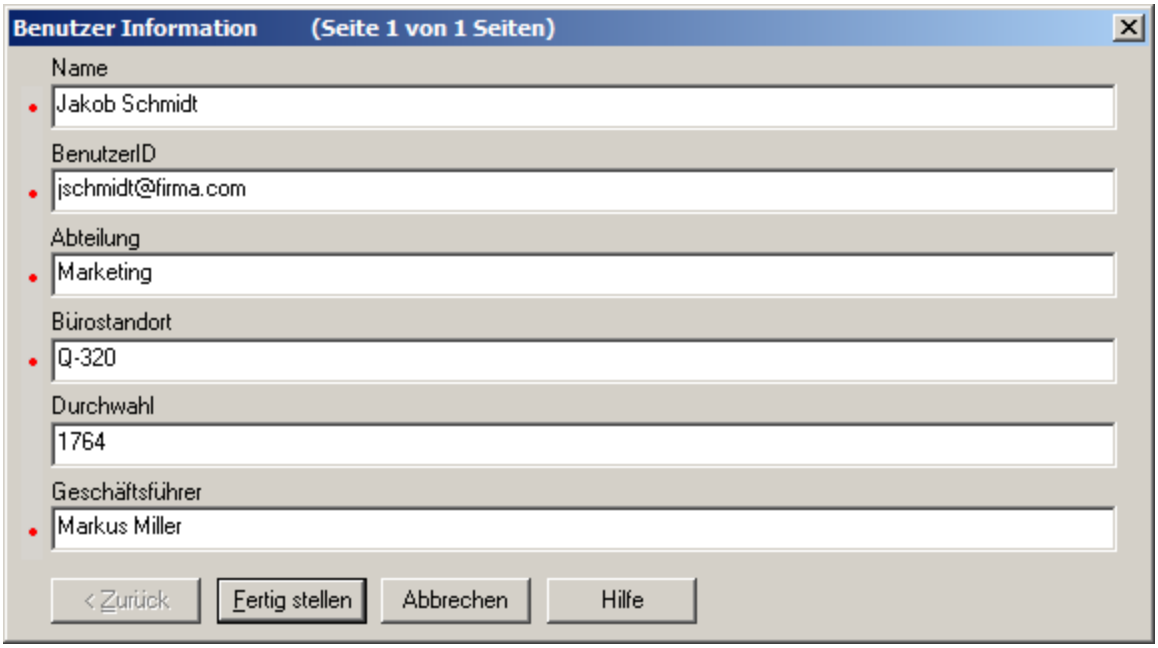
entsprechende Konfiguration in der Liste) > Benutzerdefinierte Datenformulare > Auswahl der Anzeigeoption, die Sie verwenden möchten).

Nachdem der Viewer für benutzerdefinierte Datenformulare auf dem Gerät gestartet wurde, wird eine Liste der Formulare und der Status der einzelnen Formulare angezeigt.

- **Neu:** Gibt an, dass das Formular von diesem Benutzer noch nie ausgefüllt wurde.
- **Abgeschlossen:** Gibt an, dass der Benutzer dieses Formular geöffnet und zumindest die erforderlichen Felder ausgefüllt hat.
- **Wiederholen:** Gibt an, dass der Benutzer dieses Formular bereits ausgefüllt hat, das Formular sich seither jedoch geändert hat. Der Benutzer muss sich das Formular erneut ansehen und gegebenenfalls Änderungen eingeben. Sobald dies geschehen ist, wird der Status in "Abgeschlossen" geändert.

Sobald Benutzer ein auszufüllendes Formular auswählen und auf **Öffnen** klicken, wird ein einfacher Formularassistent angezeigt. Er enthält eine Fragenliste und Felder für Antworten. Wenn die Fragen auf mehrere Seiten verteilt sind, werden die Schaltflächen "Zurück" bzw. "Weiter" zur Verfügung gestellt. Benutzer können auf **Hilfe** klicken (oder die **F1**-Taste drücken), während sich der Cursor in einem Feld befindet, um einen vom Feld **Beschreibung** im Formular-Designer generierten Hilfetext einzublenden.

Bild anzeigen/ausblenden

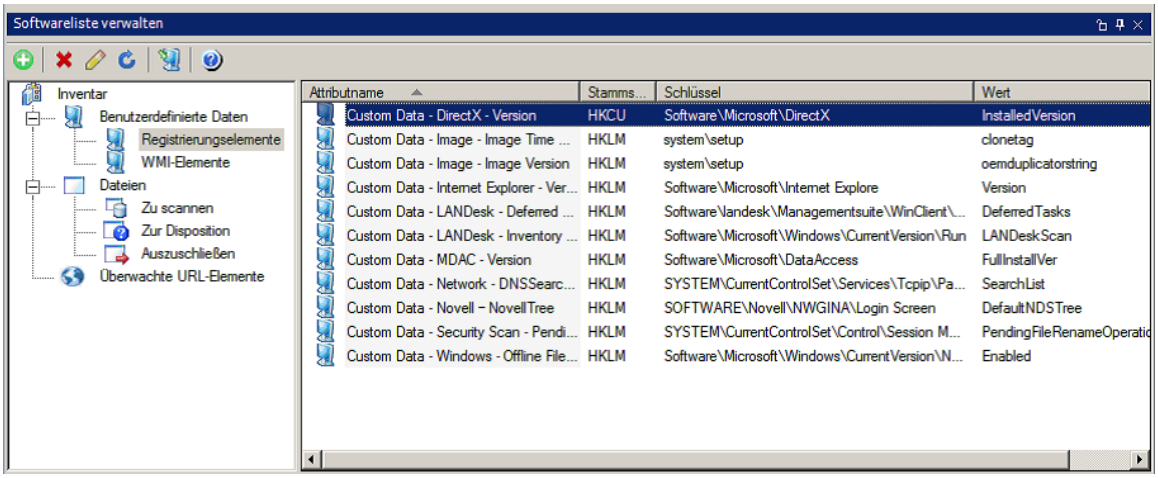


Die Benutzer müssen alle Fragen in den Pflichtfeldern beantworten, bevor sie zur nächsten Seite wechseln oder ein Formular schließen. Pflichtfelder sind mit einem roten Punkt gekennzeichnet.

Auf der letzten Seite des Formularassistenten gibt es eine **Beenden**-Schaltfläche, auf die Benutzer klicken müssen, wenn sie das Formular fertig ausgefüllt haben. Wenn die Benutzer auf diese Schaltfläche klicken, wird wieder das Dialogfeld **Formularauswahl** mit einer aktualisierten Statusmeldung neben dem Formularnamen angezeigt.

Hinzufügen von Software und Datenelementen zu Inventarscans

Das Extra **Softwareliste verwalten** verwenden Sie zum Konfigurieren der Software und der Daten, die Sie in Inventarscans einschließen möchten. Mit der von Ihnen mit diesem Extra getroffenen Auswahl bestimmen Sie die Elemente, die beim Ausführen des Inventarscanners erfasst werden.



Der Inventarscanner verwendet die von Ihnen spezifizierten Datenelemente zur Identifizierung von Softwaredateien und benutzerdefinierten Datenelementen wie Registrierungswerten, WMI-Daten und URLs. Sie können die folgenden Elemente angeben:

- **Dateien:** Dateien, die in Softwarescans enthalten sind, werden in die Liste **Zu scannen** aufgenommen. Dateien in der Liste **Auszuschließen** werden nicht in die Softwarescans eingeschlossen. Dateien in der Liste **Zur Disposition** wurden erkannt und müssen in eine der beiden anderen Listen verschoben werden.
- **Registrierungslemente:** Der Inventarscanner kann Elemente in der Windows-Registrierung auf verwalteten Geräten identifizieren. Diese Elemente werden dann in dem von Ihnen angegebenen Abschnitt der Inventarliste angezeigt.
- **WMI-Elemente:** Der Inventarscanner kann nach WMI (Windows Management Instrumentation)-Datenelementen scannen und die Ergebnisse in dem von Ihnen angegebenen Abschnitt der Inventarliste anzeigen.
- **URLs**: Der Inventarscanner kann nach URLs scannen. Dies ist bei der Verfolgung der Verwendung von webgestützten Anwendungen und von Software as a Service (SaaS) nützlich.

Die folgenden Themen bieten Informationen dazu, wie die in Inventarscans eingeschlossen Elemente geändert werden:

- "Hinzufügen oder Entfernen von Dateien für Inventarscans" auf Seite 170
- "Hinzufügen von benutzerdefinierten Registrierungselementen zu Inventarscans" auf Seite 172
- "Hinzufügen von WMI-Elementen zu Inventarscans" auf Seite 173
- "Hinzufügen von URLs zu Inventarscans" auf Seite 175

Hinzufügen oder Entfernen von Dateien für Inventarscans

Im Extra **Softwareliste verwalten** können Sie festlegen, welche Dateien in Scans eingeschlossen und welche Dateien ausgeschlossen werden.

HINWEIS: Nachdem Sie die gewünschten Elemente in der Softwareverwaltungsliste des Cores geändert haben, müssen Sie auf die Schaltfläche **Für Clients verfügbar machen** klicken, um die vom Inventarscanner verwendeten Produktdefinitionsdateien zu aktualisieren. Wenn Geräte das nächste Mal einen Inventarscan ausführen, erhält der Scanner die aktualisierten Produktdefinitionsdateien vom Coreserver und überträgt etwaige Änderungen.

Softwaredateien in Inventarscans

Der Scanner erkennt Softwareanwendungen an drei Dingen:

- Dateiname
- Dateiname und Größe
- Informationen, die in der ausführbaren Datei der Anwendung enthalten sind

Die Strukturansicht **Softwareliste verwalten** verwenden Sie, um anzugeben, welche Dateien gescannt und welche Dateien beim Inventarscan ausgeschlossenen werden sollen. Das Element **Dateien** in der Strukturansicht zeigt drei Kategorien an, die das Ordnen der Dateien vereinfachen.

- **Zu scannen:** Dateien, die der Scanner auf Geräten identifizieren wird. Diese Liste umfasst mehrere Tausend Anwendungen und stellt somit eine Grundmenge an ausführbaren Dateien bereit, die auf Ihren Geräten installiert sein können. Sie können Dateien zu dieser Liste hinzufügen oder ausschließen.
- **Zur Disposition:** Der Inventarscanner fügt die gescannten Softwaredaten zur Datenbank hinzu. Hierbei findet er auch zahlreiche Softwaredateien, die nicht erkannt werden. Diese Dateien werden zu dieser Liste hinzugefügt. Sie können Dateien aus dieser Liste in eine der beiden anderen Listen verschieben.
- **Auszuschließen:** Der Scanner ignoriert alle Instanzen einer jeden Datei, die Sie in diese Kategorie verschieben. Wenn Sie eine Datei aus **Auszuschließen** löschen, wird sie in der Kategorie **Zur Disposition** angezeigt.

Standardmäßig sucht der Inventarscanner nur nach Dateien, die unter "Softwareliste verwalten" aufgeführt sind. Die Dateien, für die "Zu scannen" oder "Auszuschließen" definiert wurde, werden in der Konfigurationsdatei für das Inventar gespeichert.

Wenn Sie alle Dateien auf den Geräten scannen möchten, können Sie den Scanmodus so einstellen, dass alle Dateien gescannt werden. Werden sämtliche Dateien in den Scan eingeschlossen, können die dabei generierten Inventarscandateien unter Umständen mehrere Megabyte groß sein. Nach dem ersten Scan übermittelt der Inventarscanner nur noch Delta-Scans, die bedeutend kleiner sind.

Nähere Informationen zum Ändern des Scanmodus und eine Beschreibung der Inventarkonfigurationsdatei finden Sie unter "Bearbeiten der LdAppl3.Template-Datei" auf Seite 178.

Scannen oder Ausschließen von Softwaredateien

Zur Bestimmung der Softwaredateien, die in den Inventarscan eingeschlossen sind, führen Sie einen der nachstehenden Tasks aus.

So schließen Sie eine Datei in einen Inventarscan ein

1. Suchen Sie die Datei in der Liste "**Zur Disposition**".
2. Ziehen Sie die Datei in die Liste "**Zu scannen**".

So schließen Sie eine Datei aus Inventarscans aus

1. Suchen Sie die Datei in der Liste "**Zur Disposition**".
2. Ziehen Sie die Datei in die Liste "**Auszuschließen**".

So schließen Sie eine Datei aus, die nicht in der Liste "Zur Disposition" zu finden ist

1. Klicken Sie auf **Auszuschließen** und klicken Sie dann auf die Schaltfläche **Hinzufügen** in der Symbolleiste.
2. Geben Sie den Namen der auszuschließenden Datei ein und klicken Sie dann auf **OK**.

So ändern Sie den Dateistatus von "Zu scannen" in "Auszuschließen"

1. Suchen Sie die Datei in der Liste "**Zu scannen**".
2. Ziehen Sie die Datei in die Liste "**Auszuschließen**".

Sie können Dateien auch aus der Liste der ausgeschlossenen Dateien in die Liste der gescannten Dateien verschieben.

Scannen von Anwendungsdateien, die keine .exe-Erweiterung aufweisen

Standardmäßig enthält die Liste **Zu scannen** Beschreibungen von ausführbaren Dateien, jedoch nur von solchen mit einer .EXE-Dateierweiterung. Wenn der Scanner auch andere Arten von Anwendungsdateien identifizieren soll (.dll, .com, .sys und so weiter), lesen Sie den Abschnitt "Bearbeiten der LdAppl3.Template-Datei" auf Seite 178.

Informationen zum Dialogfeld "Dateieigenschaften"

Dieses Dialogfeld verwenden Sie, um Dateien zur Softwareverwaltungsliste hinzuzufügen.

- **Schaltfläche "Durchsuchen":** Verwenden Sie diese Schaltfläche, um eine Datei direkt auszuwählen. Wenn eine Datei auf diese Weise ausgewählt wird, werden die Felder "Dateiname" und "Größe" automatisch ausgefüllt.
- **Dateiname:** Navigieren Sie zu einem Dateinamen oder geben Sie einen Dateinamen ein.
- **Größe (in Byte):** Geben Sie die Dateigröße in Byte an. Trennen Sie die Ziffern nicht durch Punkte oder andere Trennzeichen. Wenn Sie 1 als Dateigröße eingeben, gilt jede Datei mit diesem Dateinamen als Übereinstimmung.
- **Produktname:** Geben Sie den Namen des Produkts ein, zu dem diese Datei gehört.
- **Anbieter:** Geben Sie den Namen des Produktanbieters ein, der die Datei verwendet.
- **Version:** Geben Sie eine Versionsbezeichnung für die Datei ein.
- **Aktion oder Status:** Wählen Sie aus, was mit dieser Datei geschehen soll:
    - **Zu scannen:** Fügen Sie die Datei zu dieser Kategorie hinzu, wenn der Inventarscanner Geräte nach dieser Datei durchsuchen soll.
    - **Zur Disposition:** Fügen Sie die Datei zu dieser Kategorie hinzu, wenn Sie später entscheiden möchten, was Sie mit dieser Datei tun möchten.

Hinzufügen von benutzerdefinierten Registrierungselementen zu Inventarscans

Der Inventarscanner kann nach Registrierungsschlüsseln scannen, die Sie festlegen, und deren Werte zur Coredatenbank hinzufügen. Dies kann sich bei angepassten Softwareprodukten, Assetinformationen oder anderen Daten, die in der Registrierung gespeichert sind und in die Coredatenbank eingefügt werden sollen, als sinnvoll erweisen.

Mit dem Extra "Softwareverwaltung" können Sie Registrierungsschlüssel angeben, die zum Inventarscan hinzugefügt werden sollen. Ergebnisse werden in dem von Ihnen angegebenen Abschnitt des Inventars angezeigt.

Management Suite stellt mehrere Registrierungselemente bereit. Sie können die Eigenschaften dieser Elemente anzeigen und anhand dieser Beispiele ablesen, wie Sie solche Registrierungselemente erstellen. Um die Eigenschaften eines Elements anzuzeigen, klicken Sie mit der rechten Maustaste darauf und wählen dann **Eigenschaften** aus.

So fügen Sie einen Registrierungsschlüssel zu den Inventarscans hinzu

1. Klicken Sie auf **Extras > Berichte/Überwachung > Softwareliste verwalten**.
2. Erweitern Sie den Eintrag **Benutzerdefinierte Daten** und klicken Sie auf **Registrierungselemente**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen**.
4. Wählen Sie Daten aus und geben Sie Daten ein wie unten beschrieben.
5. Klicken Sie auf **OK**.

Folgende Daten stellen Elemente des Registrierungsscans dar:

- **Root-Schlüssel**: Wählen Sie den Typ von Registrierungsschlüssel aus, den Sie scannen möchten.

  HKLM = HKEY_LOCAL_MACHINE

  HKCC = HKEY_CURRENT_CONFIG

  HKCR = HKEY_CLASSES_ROOT

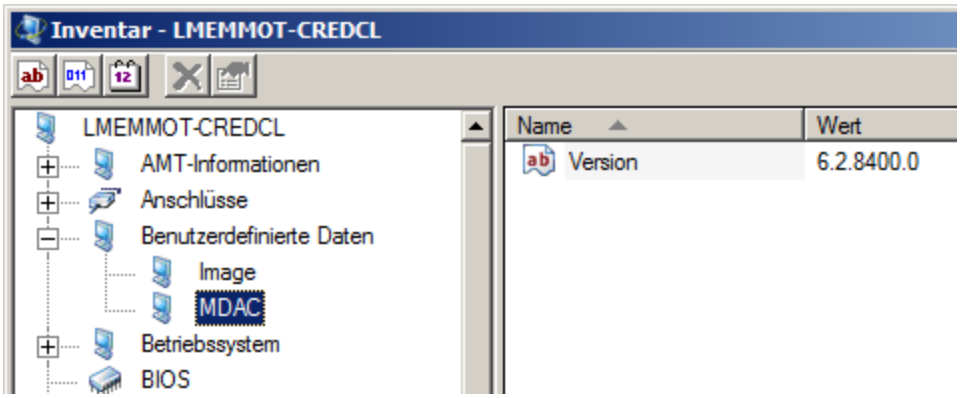
  HKU = HKEY_USERS

  HKCU = HKEY_CURRENT_USER

- **Schlüssel:** Der Pfad in der Registrierung, der den Speicherort des Schlüssels definiert. Elemente müssen mit einem umgekehrten Schrägstrich (\) getrennt werden, wobei jedes Element zwischen den umgekehrten Schrägstrichen eine Ebene in der Strukturhierarchie der Registrierung darstellt (so wie sie im Registrierungseditor angezeigt wird).
- **Wert:** Der Suchwert, nach dem der Inventarscanner sucht.
- **Attributname:** Die Beschreibung des Ortes, an dem die Daten in der Inventarstruktur angezeigt werden. Elemente werden hierarchisch geordnet angezeigt und müssen mit " - " (Leerzeichen Bindestrich Leerzeichen) getrennt eingegeben werden, damit sie im Inventar korrekt angezeigt werden. Das erste Element, das Sie hier eingeben, ist der Name der Inventarstruktur, die dann die Daten wie "Benutzerdefinierte Daten" enthält.

  Der Attributname `Benutzerdefinierte Daten - MDAC - Version` wird beispielsweise in der

Inventarzusammenfassung eines Geräts wie folgt angezeigt.



HINWEIS: Nachdem Sie die gewünschten Elemente in der Softwareverwaltungsliste des Cores geändert haben, müssen Sie auf die Schaltfläche **Für Clients verfügbar machen** klicken, um die vom Inventarscanner verwendeten Produktdefinitionsdateien zu aktualisieren. Wenn Geräte das nächste Mal einen Inventarscan ausführen, erhält der Scanner die aktualisierten Produktdefinitionsdateien vom Coreserver und überträgt etwaige Änderungen.

Hinzufügen von WMI-Elementen zu Inventarscans

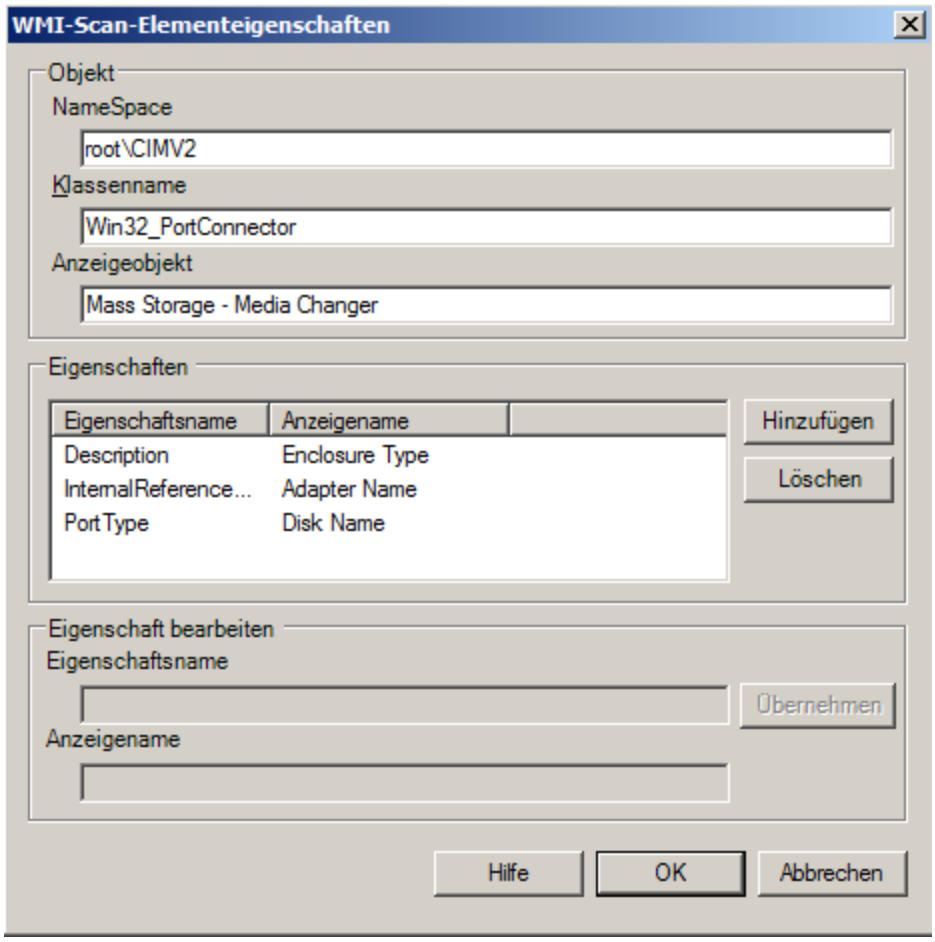
Der Inventarscanner kann nach WMI (Windows Management Instrumentation)-Datenelementen scannen und deren Werte zur Coredatenbank hinzufügen. Diese Daten werden dann in der Inventarübersicht angezeigt.

Verwenden Sie diese Option, wenn Inventarelemente für Windows-Geräte vorliegen, die Sie in der mit Management Suite gelieferten Standard-Inventarübersicht nicht finden können.

Wenn Sie WMI-Elemente zum Inventarscan hinzufügen wollen, sollten Sie mit den WMI-Klassen und -Instanzen vertraut sein und auch wissen, zu welchem Namespace eine Klasse gehört. Verwenden Sie ein Tool wie Microsoft CIM Studio oder PowerShell (in Windows 7), um die WMI-Klassen zu durchsuchen.

Bei jeder Klasse können Sie nach einer oder mehreren Eigenschaften scannen und diese Werte in die Inventarstruktur zurückgeben.

Das folgende Beispiel ist eine WMI-Klasse für einen Medienportanschluss. Sie umfasst drei Eigenschaften. Der Namespace, die Klasse und der Inventaranzeigepfad werden im oberen Abschnitt des Dialogfelds definiert. Die Eigenschaften werden einzeln hinzugefügt und allesamt in der Mitte des Dialogfelds im Feld **Eigenschaften** aufgelistet.



Nachdem dieses benutzerdefinierte Datenelement definiert ist und durch Klicken auf die Symbolleisten-Schaltfläche **Für Clients verfügbar machen** für verwaltete Geräte verfügbar gemacht wurde, wird ein verwaltetes Gerät, das einen Medienportanschluss besitzt, dieses Element in der Inventarübersicht auflisten. In der Inventarstruktur wird das Element unter Massenspeicher > Medienwechsler aufgeführt. Drei Datenelemente werden angezeigt: Adaptername, Plattenname und Gehäusetyp.

So fügen Sie ein WMI-Element zu den Inventarscans hinzu

1. Klicken Sie auf **Extras > Berichte/Überwachung > Softwareliste verwalten**.
2. Erweitern Sie den Eintrag **Benutzerdefinierte Daten** und klicken Sie auf **WMI-Elemente**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen**.
4. Geben Sie **Objekt**daten wie nachstehend beschrieben ein.
5. Klicken Sie auf **Hinzufügen**, um eine Eigenschaft hinzuzufügen. Geben Sie einen **Eigenschaftennamen** und einen **Anzeigenamen** wie nachstehend beschrieben ein. Klicken Sie auf **Übernehmen**, um die Eigenschaft hinzuzufügen.
6. Wenn alle Daten vollständig sind, klicken Sie auf **OK**.

Folgende Daten stellen WMI-Elemente dar:

- **NameSpace**: Der WMI-Namespace. Dieser lautet üblicherweise `root\\CIMV2`, es kann aber auch ein anderer Namespace sein.

- **Klassenname:** Der WMI-Klassenname.
- **Anzeigeobjekt:** Die Beschreibung des Ortes, an dem die Daten in der Inventarstruktur angezeigt werden. Elemente werden hierarchisch geordnet angezeigt und müssen mit " - " (Leerzeichen Bindestrich Leerzeichen) getrennt eingegeben werden, damit sie im Inventar korrekt angezeigt werden. Das erste Element, das Sie hier eingeben, ist der Name der Inventarstruktur, die dann die Daten wie "Benutzerdefinierte Daten" enthält.

Jedes Element kann eine oder mehrere Eigenschaften aufweisen, nach denen der Scanner sucht.

- **Eigenschaftenname:** Der Name, der die WMI-Eigenschaft identifiziert.
- **Anzeigename:** Der Name, der zur Identifizierung der WMI-Eigenschaft in der Inventarstruktur verwendet wird. Dieser Name erscheint in der Inventarstruktur auf der ersten Ebene unterhalb des Anzeigeobjekts.

HINWEIS: Nachdem Sie die gewünschten Elemente in der Softwareverwaltungsliste des Cores geändert haben, müssen Sie auf die Schaltfläche **Für Clients verfügbar machen** klicken, um die vom Inventarscanner verwendeten Produktdefinitionsdateien zu aktualisieren. Wenn Geräte das nächste Mal einen Inventarscan ausführen, erhält der Scanner die aktualisierten Produktdefinitionsdateien vom Coreserver und überträgt etwaige Änderungen.

Hinzufügen von URLs zu Inventarscans

Der Inventarscanner kann nach URLs scannen. Dies ist bei der Verfolgung der Verwendung von webgestützten Anwendungen und von Software as a Service (SaaS) nützlich.

Zu jeder URL, die Sie hinzufügen, speichert der Inventarscanner Daten wie beispielsweise:

- wie oft die URL besucht wird
- wieviel Zeit auf das Anzeigen von Seiten unter dieser URL verwendet wurde
- Datum und Uhrzeit, zu der die URL besucht wurde

So fügen Sie eine URL zu den Inventarscans hinzu

1. Klicken Sie auf **Extras > Berichte/Überwachung > Softwareliste verwalten**.
2. Klicken Sie auf **Überwachte URL-Elemente**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Hinzufügen**.
4. Geben Sie einen Domänennamen in das Feld **URL** ein.

Sie können einen Domänennamen mit Unterdomänen eingeben, die durch Punkte getrennt sind, aber Sie können keine spezifischen Pfade einschließen. Der Domänenname darf keine ungültigen Zeichen enthalten. Wenn Sie einen Pfad oder ungültige Zeichen eingeben, wird eine Fehlermeldung angezeigt und Sie müssen den Fehler in der URL beheben.

Sie können bis zu 10 Unterdomänenebenen einschließen, die maximal 60 Zeichen pro Ebene aufweisen dürfen. Die Gesamtzahl der Zeichen im Domänenname darf 260 Zeichen nicht überschreiten.

HINWEIS: Nachdem Sie die gewünschten Elemente in der Softwareverwaltungsliste des Cores geändert haben, müssen Sie auf die Schaltfläche **Für Clients verfügbar machen** klicken, um die vom Inventarscanner verwendeten Produktdefinitionsdateien zu aktualisieren. Wenn Geräte das nächste Mal einen Inventarscan ausführen, erhält der Scanner die aktualisierten Produktdefinitionsdateien vom

Coreserver und überträgt etwaige Änderungen.

Ändern von Parametern für Inventarscans

Dieses Thema beschreibt verschiedene Wege zur Änderung der Parameter für Inventarscans. Es bietet die folgenden Informationen:

- "Scannen von benutzerdefinierten Informationen" auf Seite 176
- "Festlegen von Intervall und Verlauf des Softwarescannens" auf Seite 176
- "Scannerbefehlszeilenparameter" auf Seite 177
- "Bearbeiten der LdAppl3.Template-Datei" auf Seite 178
- "Hinzufügen von BIOS-Textzeichenfolgen zur Coredatenbank" auf Seite 180

Scannen von benutzerdefinierten Informationen

Der Windows-Inventarscanner überprüft die Registrierung des Geräts automatisch auf benutzerdefinierte Daten. Wenn Sie ein Gerät konfigurieren, werden folgende Schlüssel in der Registrierung installiert:

- HKEY_LOCAL_MACHINE\SOFTWARE\INTEL\LANDESK\INVENTORY\CUSTOM FIELDS

Der Inventarscanner scannt stets die Registrierung nach dem Schlüssel "Custom Fields" und nimmt die Daten auf, die er unter diesem Schlüssel findet. Anschließend gibt er diese benutzerdefinierten Daten in die "Benutzerdefiniert"-Felder der Coredatenbank ein. Welche Informationen in den Schlüsseln "Custom Fields" stehen sollen, können Sie je nach Ihren Anforderungen selbst entscheiden. In der Konsole werden diese Daten in den "Benutzerdefiniert"-Feldern angezeigt.

Der Inventarscanner liest zwei Datentypen:

- REG_SZ
- REG_DWORD

HINWEIS: Unterschlüssel für "Benutzerdefiniert"-Felder
Der Inventarscanner sucht nicht nach Unterschlüsseln unterhalb der "Benutzerdefiniert"-Felder.

HINWEIS: Zeichenfolgelänge der "Benutzerdefiniert"-Felder
ASCII-Zeichenfolgen dürfen maximal 255 Zeichen enthalten. Mehrbyte-Zeichensatz (MBCS)-Zeichenfolgen müssen eine Länge zwischen 127 und 255 Zeichen haben.

Festlegen von Intervall und Verlauf des Softwarescannens

Sie können festlegen, wann die Software eines Geräts gescannt wird und wie lange das Verlaufsprotokoll der Inventaränderungen auf dem Coreserver gespeichert bleibt. Diese Intervalle gelten für jedes Gerät.

HINWEIS: Die *Hardware* eines Geräts wird jedes Mal gescannt, wenn das Gerät gestartet und mit dem Netzwerk verbunden wird.

So legen Sie Einstellungen für das Softwarescannen fest

1. Klicken Sie in der Netzwerkansicht der Konsole auf **Konfigurieren > Dienste > Inventar > Software**.
2. Legen Sie die Häufigkeit der Softwareprüfung fest.
3. Legen Sie fest, wie viele Tage das Verlaufsprotokoll gespeichert werden soll.

HINWEIS: Der Coreserver und die Softwareprüfung
Diese Funktion gilt nur für Geräte. Der Coreserver ist nicht betroffen, da er grundsätzlich täglich gescannt wird.

Scannerbefehlszeilenparameter

Sie können Befehlszeilenparameter zu den Kontexteigenschaften des Inventarscanners (ldiscn32.exe) hinzufügen, um ihn zu steuern.

Die nachstehende Tabelle enthält eine Aufstellung der Befehlszeilenparameter für den Scanner:

Option	Beschreibung
/NTT=IP	IP-Adresse des Coreservers oder DNS-Name und UDP-Port. Zum Beispiel: /NTT=123.123.123.123:5007 oder /NTT=CORESERVER:5007.
/UDP	Scanner kommuniziert über UDP statt über TCP. Kombinieren Sie diesen Schalter mit /NTT=[IP].
/NOUI	Erzwingt die Scannerausführung ohne Benutzeroberfläche.
/i=inifile	Gibt den Pfad (HTTP, UNC) oder einen Laufwerksbuchstaben für die Master-LdAppl3-Datei an. ldiscn32.exe kopiert außerdem die LdAppl3-Datei, die an diesem Speicherort gefunden wurde, in die localLdAppl3.ini-Datei des Geräts. Die Scanner vergleichen das Datum der Master-LdAppl3-Datei mit der lokalen LdAppl3.ini-Datei. Wenn die Daten nicht übereinstimmen, wird die Masterdatei lokal kopiert.
/d=Verzeichnis	Startet den Softwarescan im angegebenen Verzeichnis. Standardmäßig wird das Scannen im Root-Verzeichnis der jeweiligen lokalen Festplatte gestartet.
/L	Die Scanergebnisse werden an den Coreserver gesendet, von dem aus das Gerät konfiguriert wurde. Wenn Sie /L verwenden, ist der Parameter /NTT überflüssig.
/sync	Erzwingt einen vollständigen Scan, einschließlich eines vollständigen Softwarescans. Vollständige Scandateien können auf eine Größe von mehreren MB anwachsen.
/n	Durchsucht keine Unterverzeichnisse.

Option	Beschreibung
/v	Ausführlicher Modus.
/Z=Zahl der Wiederholungsversuche	Gibt an, wie oft der Scanner versuchen wird, den Scan neu zu senden.
/W=Wartezeit in Sekunden	Festgelegte Wartezeit des Scanners in Sekunden, bevor das Scannen gestartet wird.
/? oder /h	Zeigt die Hilfe zur Befehlszeilensyntax an.
/s=Servername	Legt den Coreserver fest, auf dem Inventardaten gespeichert werden.
/f oder /f-	Erzwingt einen Softwarescan, unabhängig vom Scanintervall, das an der Konsole festgelegt wurde. Geben Sie /f- an, um einen Softwarescan zu deaktivieren, unabhängig vom Scanintervall, das an der Verwaltungskonsole festgelegt wurde.
/t=[path]filename	Kopiert den Inhalt der angegebenen Datei in die Coredatenbank. Verwenden Sie diese Option, um Inventardaten von eigenständigen Geräten oder von separaten Inventardateien einzugeben.
/o=[path]filename	Schreibt Inventardaten in die festgelegte Ausgabedatei.
/m	Erstellt eine nicht nach dem Unicode-Standard formatierte ldiscan.mif-Datei im Verzeichnis C:/DMI/DOS/MIFS. Diese Datei enthält die Inventardaten, die während des Scannens gefunden wurden.
/muni	(Nur ldiscn32.exe) Erstellt eine Unicode-ldiscan.mif-Datei in dem Verzeichnis, das im MIFPATH der LdAppl3.ini-Datei gefunden wurde. Diese Datei enthält die Inventardaten, die während des Scannens gefunden wurden.
/do16	Aktiviert den 16-Bit-Inventarscanner (INV16.EXE) auf verwalteten Geräten.

Bearbeiten der LdAppl3.Template-Datei

Informationen zur den Scanner-Inventarparametern sind in der Datei LdAppl3.Template enthalten. Diese Vorlagendatei erkennt zusammen mit der Datei LdAppl3 das Softwareinventar eines Geräts.

Sie können den Abschnitt [LANDesk Inventar] der Vorlagendatei bearbeiten, um die Parameter zu konfigurieren, die festlegen, wie der Scanner das Softwareinventar erkennt. Standardmäßig ist LdAppl3.Template im folgenden Verzeichnis auf dem Coreserver gespeichert:

- \Programme\LANDesk\ManagementSuite\LDLogon

Diese Tabelle unterstützt Sie beim Bearbeiten des Abschnitts [LANDesk Inventar] in einem Texteditor.

Option	Beschreibung
Modus	Bestimmt, wie der Scanner auf den Geräten nach Software scannt. Standard ist "Aufgelistete". Es gibt folgende Einstellungen: • **Aufgelistete:** Zeichnet die Dateien auf, die in LdAppl3 aufgeführt sind. • **Nicht aufgelistete:** Zeichnet Name und Datum aller Dateien auf, deren Erweiterungen in der Zeile "ScanExtensions" aufgeführt, jedoch nicht in LdAppl3 definiert sind. Mit dieser Methode lässt sich nicht autorisierte Software auf dem Netzwerk finden. • **Alle:** Findet Dateien, die über Erweiterungen verfügen, die in der Zeile "ScanExtensions" aufgelistet sind.
Duplikat	Zeichnet Mehrfachinstanzen von Dateien auf. Setzen Sie den Wert auf OFF, um nur die erste Instanz aufzuzeichnen, oder auf ON, um alle gefundenen Instanzen aufzuzeichnen. Standard ist ON.
ScanExtensions	Legt die Dateierweiterungen fest (.exe, .com, .cfg usw.), nach denen gescannt wird. Trennen Sie die Erweiterungen durch ein Leerzeichen voneinander. Standardmäßig werden nur .exe-Dateien gescannt.
Version	Die Versionsnummer der Datei LdAppl3.
Revision	Die Revisionsnummer der Datei LdAppl3, die für zukünftige Kompatibilität sorgt.
CfgFiles 1-4	Zeichnet Datum, Uhrzeit, Dateigröße und Inhalt der entsprechenden Dateien auf. Lassen Sie den Laufwerksbuchstaben (z. B. c:) weg, wenn Sie alle lokalen Laufwerke durchsuchen wollen. Sie können mehr als eine Datei auf jeder der vier Zeilen angeben. Die Länge der Zeilen ist jedoch auf 80 Zeichen beschränkt. Trennen Sie Pfadnamen innerhalb derselben Zeile durch ein Leerzeichen voneinander ab. Der Scanner vergleicht die Daten und die Größe der aktuellen Datei mit der des vorherigen Scans. Wenn Datum und Größe nicht übereinstimmen, zeichnet der Scan den Inhalt der Datei als neuere Revision auf.
ExcludeDir 1-3	Schließt bestimmte Verzeichnisse aus einem Scan aus. Lassen Sie den Laufwerksbuchstaben (z. B. c:) weg, wenn Sie alle lokalen Laufwerke ausschließen wollen. Aufzählungen müssen mit 1 beginnen und fortlaufend sein. Sie können Umgebungsvariablen in folgendem Format verwenden: "%varname%". Sie können eine Platzhalterzeichen (*) nur in einem "beginnt mit"-Format verwenden (ExcludeDir=%windir%\$NtUninstall*\ ). Sie müssen jede Zeile mit "\" beenden.
MifPath	Legt fest, wo MIF-Dateien auf dem lokalen Laufwerk eines Geräts gespeichert werden. Der Standardpfad ist c:\DMI\DOS\MIFS.

Option	Beschreibung
UseDefaultVersion	Wenn die Einstellung TRUE gewählt wird, meldet der Scanner nur dann eine Übereinstimmung, wenn eine Datei genau mit einem Dateinamens- und Dateigrößeneintrag in LdAppl3 übereinstimmt (in der Meldung trägt die Version den Namen EXISTS). Dies kann zu falschen Ergebnissen für Anwendungen führen, die einen allgemeinen Dateinamen mit einer unbekannten Anwendung gemeinsam verwenden. In der ursprünglichen Datei LdAppl3.Template ist dieser Parameter auf FALSE festgelegt; d. h., es wird nur dann ein Eintrag hinzugefügt, wenn es sich um eine genaue Übereinstimmung handelt. Wenn der Parameter fehlt, ist die Standardeinstellung TRUE.
SendExtraFileData	Wenn die Einstellung TRUE lautet, werden zusätzliche Dateidaten an den Coreserver gesendet. Standard ist FALSE. Dies bedeutet, dass standardmäßig nur Pfad, Name und Version in die Coredatenbank eingetragen werden.

Verfügbarmachen von Inventarscanänderungen für Clients

Wenn Sie Änderungen an der LdAppl3.Template-Datei vornehmen, müssen Sie diese Änderungen für verwaltete Geräte bereitstellen, damit die Art und Weise der Ausführung des Inventarscans geändert wird. Die Änderungen werden übernommen, wenn der Befehlszeilenparameter /i des Scanners auf Ihren verwalteten Geräten verwendet wird.

So bearbeiten Sie die Datei LdAppl3.Template

1. Wechseln Sie vom Coreserver in das Verzeichnis "LDLogon" und öffnen Sie LdAppl3.Template in Notepad oder einem anderen Texteditor.
2. Blättern Sie nach unten zu dem Parameter, den Sie aktualisieren möchten, und nehmen Sie die Änderungen vor.
3. Speichern Sie die Datei.

So stellen Sie Scanänderungen für verwaltete Geräte bereit

1. Bearbeiten und speichern Sie die LdAppl3.Template-Datei.
2. Klicken Sie in der Konsole auf **Extras > Berichte/Überwachung > Softwareliste verwalten**
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Für Clients verfügbar machen**, damit den Geräten die neuesten Änderungen zur Verfügung stehen, wenn diese das nächste Mal einen Inventarscan durchführen.

Hinzufügen von BIOS-Textzeichenfolgen zur Coredatenbank

Die Datei LdAppl3.Template enthält den Abschnitt [BIOS Info]. Dieser Abschnitt ermöglicht das Suchen nach Informationen im BIOS eines Computers. Sie können einen oder mehrere Einträge in den Abschnitt [BIOS Info] einfügen. Diese Einträge definieren neue Schlüssel in der Coredatenbank und liefern Parsing-Anweisungen an den Inventarscanner. Mit den Parsing-Anweisungen wird festgelegt, wo in der LDBIOS.TXT nach einer bestimmten Zeichenfolge gesucht werden soll. Mithilfe dieser Anweisungen fügt der Inventarscanner Zeichenfolgen aus der LDBIOS.TXT-Datei in die Coredatenbank ein.

Der Inventarscanner verwendet eine Parsing-Methode zum Auffinden von BIOS-Informationen. So können Sie nach Informationen suchen, die sich eine oder mehrere Zeilen über oder unter einer angegebenen Textzeichenfolge befinden. Mit einer solchen Suche können Sie nach beliebigen Buchstaben- und Zahlenkombinationen suchen, die Computerhardware zugewiesen sind.

Textzeichenfolgen in LDBIOS.TXT

Wenn Sie den Inventarscan mit dem Befehlszeilenparameter /do16 ausführen, werden die im BIOS verfügbaren Textzeichenfolgen während eines Inventarscans in eine Textdatei namens LDBIOS.TXT exportiert. In LDBIOS.TXT werden alle Zeichenfolgen gespeichert, die vom Scanner erstellt werden. Wenn Sie diese Informationen in der Datenbank speichern möchten, können Sie sie mithilfe des CFGFILES-Parameters in der Datei LdAppl3.ini als Konfigurationsdatei speichern.

Beispiel von BIOS-Einträgen in der Datei LdAppl3.Template

Das folgende Beispiel wurde dem [BIOS Info]-Abschnitt der Datei LdAppl3.Template entnommen:

```
[BIOS Info]
StringLength=4
Key = BIOS - Manufacturer
Parameters = AllValues,FirstInstance
Value = AMI|American Megatrends::AMI::BIOS - AMI
Value = Copyright.*Dell::Dell::BIOS - Dell
[BIOS - AMI]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(.*\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*\(AMI|American Megatrends\)
[BIOS - Dell]
Key = % - Version
Parameters = FirstValue,FirstInstance
Value = BIOS Version \(A.+\)::\1
Value = BIOS Version: \(A.+\)::\1
Key = % - Copyright Notice
Parameters = AllValues,AllInstances
Value = ©.*Dell|[Cc]opyright.*Dell
```

Erläuterungen zu BIOS-Einträgen

Einträge im Abschnitt [BIOS Info] setzen sich wie folgt zusammen:

- **[Abschnitsname]** Identifiziert eine neue Komponente in der Coredatenbank.
- **StringLength=** Gibt die Mindestlänge der zu suchenden Zeichenfolgen an.
- **Key=** Identifiziert Klasse und Attributnamen der beim Durchsuchen der LDBIOS.TXT-Datei zurückgegebenen Informationen.
- **Parameters=** Legt die Suchkriterien fest, die dem Scanner mitteilen, wo und wie nach Werten gesucht werden soll, die einem bestimmten Schlüssel zugeordnet sind.
- **Value=** Gibt den Wert an, der im BIOS gesucht wird. Ein Wert besteht aus drei Teilen, die jeweils durch zwei Doppelpunkte getrennt sind (::). Bei diesen Werten ist die Groß-/Kleinschreibung zu beachten. Alle Zeichen im Wert, selbst Leerzeichen, werden bei der Suche berücksichtigt, sofern es sich nicht um einen Operator handelt.

Zusätzliche Inventartasks und Fehlerkorrektur

Dieses Thema enthält zusätzliche Informationen zum Inventarscannen sowie einige Tipps zur Fehlerbehebung. Es bietet die folgenden Informationen:

- "Planen eines Inventarscan-Tasks" auf Seite 182
- "Scannen von Einzelgeräten" auf Seite 182
- "Hinzufügen von Inventardatensätzen zur Coredatenbank" auf Seite 183
- "Erstellen von MIF-Dateien" auf Seite 183
- "Scannen nach benutzerdefinierten Daten auf Macintosh-Geräten" auf Seite 183
- "Fehlerbehebung beim Inventarscanner" auf Seite 187

Planen eines Inventarscan-Tasks

Wenn ein Gerät die Management Suite-Agenten ausführt, können Sie ein Skript planen, das einen Inventarscan auf dem Gerät initiiert.

So planen Sie einen Inventarscan

1. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Inventarscan planen** .
3. Konfigurieren Sie im Fenster **Geplante Tasks** Ziele und Startzeit des Tasks.

Das Inventarscan-Skript befindet sich im Verzeichnis \Programme\LANDesk\ManagementSuite\Scripts. Das Skript ist eine Windows-.INI-Datei, die Sie mit einem beliebigen Texteditor bearbeiten können. Wenn Sie die Optionen oder Parameter in diesem Skript ändern möchten, öffnen Sie es, und befolgen Sie die darin beschriebenen Anweisungen.

Scannen von Einzelgeräten

So scannen Sie ein Einzelgerät

1. Kopieren Sie das entsprechende Inventarscanner-Tool und eine Softwarebeschreibungsdatei (in der Regel LdAppl3.ini) auf eine Diskette oder einen USB-Speicherstick. (Möglicherweise müssen Sie auch elogapi.dll, ygrep32.dll, locv16vc0.dll, inv16.exe, loc32vc0.dll, ltapi.dll und ldiscn32.exe kopieren.)
2. Scannen Sie mithilfe von **/O= Parameter** und legen Sie dabei den Pfad und den Dateinamen der Ausgabedatei fest.
3. Geben Sie in der Befehlszeilenaufforderung einen **eindeutigen Namen** für das Gerät ein. Dieser Name wird im Beschreibungsfeld in der Coredatenbank angezeigt. Zum Beispiel:

```
ldiscn32.exe /f /v /o=c:\%Computername%.scn
```

4. Kopieren Sie die hierbei erstellte Scandatei in das Verzeichnis ...\ManagementSuite\ldscan des Coreservers, damit diese zur Datenbank hinzugefügt wird.

So scannen Sie ein Gerät mit Netzwerkzugriff auf den Coreserver

1. Nehmen Sie eine Laufwerkszuordnung zu dem ldlogon-Verzeichnis auf dem Coreserver vor, in dem der Scan erscheinen soll.
2. Klicken Sie auf **Start > Ausführen** und fügen Sie den folgenden Befehl ein:

```
N:\LDISCN32.EXE /NTT=CORESERVERNAME:5007 /S="CORESERVERNAME"
/I=HTTP://CORESERVERNAME/ldlogon/ldappl3.ldz /V /F /SYNC
```

Hinzufügen von Inventardatensätzen zur Coredatenbank

Sie können Inventardaten von einem Einzelgerät oder separaten Inventardateien hinzufügen, indem Sie das Inventarscanner-Tool von der Befehlszeile des Betriebssystems ausführen.

So fügen Sie Inventardatensätze aus einer Datei in die Coredatenbank ein

- Führen Sie den Scanner mit den Parametern /S= , /T= und /NTT= aus.

Erstellen von MIF-Dateien

Wenn Sie eine MIF-Datei benötigen, in der die Inventardaten eines Geräts gespeichert werden, können Sie sie erstellen, indem Sie den entsprechenden Scanner in der Befehlszeile ausführen.

Um eine Unicode-MIF-Datei zu erstellen, verwenden Sie die Option /MUNI. Um eine MIF-Datei zu erstellen, die nicht im Unicode-Format vorliegt, verwenden Sie die Option /M.

So erstellen Sie MIF-Dateien

- Geben Sie Folgendes an einer DOS-Eingabeaufforderung ein:

```
LDISCN32/MUNI/V
```

Scannen nach benutzerdefinierten Daten auf Macintosh-Geräten

Sie können Kundendaten von Geräten erfassen, auf denen der LANDesk Agent für Macintosh ausgeführt wird, und ins Inventar einarbeiten. Die Informationen werden in XML-Dateien in einem bestimmten Verzeichnis auf dem Clientgerät gespeichert. Die nachstehend aufgeführten Informationen verwenden Sie, um XML-Dateien mit benutzerdefinierte Daten am richtigen Speicherort für die Verarbeitung ins Inventar zu erstellen.

Informationen zu alternativen Lösungen für benutzerdefinierte Daten für Macintosh finden Sie im Whitepaper "Macintosh Agent Custom Data", das hier zum Download zur Verfügung steht: http://community.landesk.com/support/docs/DOC-1570.

HINWEIS: Die Implementierung von benutzerdefinierten Daten mit dem LANDesk Agenten für Macintosh verwendet keine benutzerdefinierten Datenformulare. Tasks mit benutzerdefinierten Datenformularen können nicht erfolgreich für Geräte bereitgestellt werden, auf denen der LANDesk Agent für Macintosh ausgeführt wird.

XML-Dateien mit benutzerdefinierten Daten

Bevor Sie benutzerdefinierten Daten zu einem Inventarscan von einem Gerät hinzufügen können, auf dem der LANDesk Agent für Macintosh ausgeführt wird, müssen Sie zunächst eine XML-Datei mit benutzerdefinierten Daten im korrekten Format erstellen. Dieser Abschnitt beschreibt das korrekte Dateiformat, das eine XML-Datei mit benutzerdefinierten Daten aufweisen muss, damit sie ohne Fehler verarbeitet werden kann.

Regeln für XML-Dateien mit benutzerdefinierten Daten

Für XML-Dateien, die zur Speicherung benutzerdefinierter Daten verwendet werden, gelten die folgenden Regeln. XML-Dateien mit benutzerdefinierten Daten, die nicht allen Regeln entsprechen, werden nicht verarbeitet und in das Inventar übernommen.

- XML-Dateien mit benutzerdefinierten Daten können einen beliebigen Namen aufweisen, müssen aber die Erweiterung .xml aufweisen. Zum Beispiel:

```
Telefonnummern.xml
```

- Die erste Zeile einer XML-Datei mit benutzerdefinierten Daten muss eine XML-Deklaration enthalten. Zum Beispiel:

```
<?xml version="1.0" encoding="UTF-8"?>
```

- Alle Starttags innerhalb einer XML-Datei mit benutzerdefinierten Daten müssen einen entsprechenden Endtag besitzen. Zum Beispiel:

```
<privat>(0123) 456789</privat>
```

- Tags innerhalb einer XML-Datei dürfen allesamt keine Leerzeichen aufweisen. Zum Beispiel:

```
<Telefonnummer_1></Telefonnummer_1>
```

- Alle Elemente innerhalb eine XML-Datei mit benutzerdefinierten Daten, die eine einzelne Informationszeile darstellen, müssen in ein übergeordnetes Element eingeschlossen sein. Zum Beispiel:

```
<Telefonnummern><privat>(0123) 456789</privat></Telefonnummern>
```

- Für den Fall, dass ein Element in einer XML-Datei mit benutzerdefinierten Daten keinen Inhalt aufweist, wird der Elementname nicht als benutzerdefiniertes Datenelement im Inventar angezeigt. Zum Beispiel:

```
<privat></privat>
```

- Für den Fall, dass keines der Elemente, die in ein übergeordnetes Element in einer XML-Datei mit benutzerdefinierten Daten geschachtelt sind, irgendeinen Inhalt aufweist, wird der Name des übergeordneten Elements nicht als Knoten unter den benutzerdefinierten Daten im Inventar angezeigt. Zum Beispiel:

```
<Telefonnummern><privat></privat><geschäftlich></geschäftlich></Telefonnummern>
```

XML-Dateien mit benutzerdefinierten Daten und einem einzelnen Eintrag

XML-Dateien mit benutzerdefinierten Daten können so erstellt werden, dass ein einziger Eintrag in den Bereich für benutzerdefinierte Daten des Inventars eingefügt wird. Zu diesem Zweck müssen die Tags jedes Elements in einer XML-Datei mit benutzerdefinierten Daten mit der Zeichenfolge benannt werden, die im Inventar angezeigt werden soll. Anschließend muss der Elementsatz in übergeordnete Elemente mit Tags geschachtelt werden, die die Zeichenfolge darstellen, die unter den benutzerdefinierten Daten in der Baumansicht des Inventars angezeigt wird.

Beispiel: Würde eine XML-Datei mit benutzerdefinierten Daten zur Erfassung von Telefonnummern verwendet, dann würde sich daraus im Inventardatensatz das nachstehend gezeigte Format ergeben:

```
<?xml version="1.0" encoding="UTF-8"?>
<Telefonnummern>
<geschäftlich>(0123) 456789 </geschäftlich>
<mobil>(0123) 456789</mobil>
<privat>0123456789</privat>
<sonstige>nicht zutreffend</sonstige>
<bevorzugte_Nummer>geschäftlich</bevorzugte_Nummer>
</Telefonnummern>
```

XML-Dateien mit benutzerdefinierten Daten und mehreren Einträgen

XML-Dateien mit benutzerdefinierten Daten können so erstellt werden, dass mehrere Einträge in den Bereich für benutzerdefinierte Daten des Inventars eingefügt werden. Zu diesem Zweck müssen die Tags jedes Elements in einer XML-Datei mit benutzerdefinierten Daten mit der Zeichenfolge benannt werden, die im Inventar angezeigt werden soll. Anschließend muss jeder Elementsatz in übergeordnete Elemente mit Tags geschachtelt werden, die die Zeichenfolge darstellen, die unter den benutzerdefinierten Daten in der Baumansicht des Inventars angezeigt wird.

Beispiel: Würde eine XML-Datei mit benutzerdefinierten Daten zur Erfassung von Mitarbeiterdaten verwendet, dann würde sich daraus im Inventardatensatz das nachstehend gezeigte Format ergeben:

```
<?xml version="1.0" encoding="UTF-8"?>
<Telefonnummern>
<geschäftlich>(0123) 456789 </geschäftlich>
<mobil>(0123) 456789</mobil>
<privat>0123456789</privat>
<sonstige>nicht zutreffend</sonstige>
<bevorzugte_Nummer>geschäftlich</bevorzugte_Nummer>
</Telefonnummern>
<Adressen>
<Adresse_geschäftlich_1>Lindenallee 123</Adresse_geschäftlich_1>
<Adresse_geschäftlich_2>Suite 550</Adresse_geschäftlich_2>
<Adresse_geschäftlich_3></Adresse_geschäftlich_3>
<Ort_geschäftlich>Frankfurt am Main </Ort_geschäftlich>
<Bundesland_geschäftlich>Hessen</Bundesland_geschäftlich>
<PLZ_geschäftlich>60528</PLZ_geschäftlich>
<Adresse_privat_1>Ulmenweg 123</Adresse_privat_1>
<Adresse_privat_2></Adresse_privat_2>
<Adresse_privat_3></Adresse_privat_3>
<Ort_privat>Frankfurt am Main </Ort_privat>
<Bundesland_privat>Hessen</Bundesland_privat>
<PLZ_privat>60528</PLZ_privat>
</Adressen>
<Mitarbeiterdaten>
<Titel>Außendienstmitarbeiter</Titel>
<Personalnummer>4562</Personalnummer>
<Manager>Robert Schmidt</Manager>
<E-Mail>Karl.Mustermann@WidgetsUndMehr.de</E-Mail>
</Mitarbeiterdaten>
```

Benutzerdefiniertes Datenverzeichnis

Jede XML-Datei mit benutzerdefinierten Daten, die ins Inventar übernommen werden soll, muss im Verzeichnis für benutzerdefinierte Daten gespeichert werden. Dieses befindet sich auf jedem Gerät, auf dem der LANDesk Agent für Macintosh ausgeführt wird, unter **/Library/Application Support/LANDesk/CustomData**.

Nachdem eine XML-Datei mit benutzerdefinierten Daten ins Inventar abgearbeitet wurde, verbleibt die Datei im Verzeichnis "CustomData". Auf diese Weise können im Anschluss daran durchgeführte vollständige Scans (und Deltascans, bei denen **Softwarescan erzwingen** aktiviert ist) auch die Informationen aus XML-Dateien mit benutzerdefinierten Daten einbeziehen, die im benutzerdefinierten Datenverzeichnis gespeichert sind.

Inventar

Während des Softwareteils eines Inventarscans wird das Verzeichnis "CustomData" geprüft. Alle XML-Dateien im Verzeichnis "CustomData" werden in benutzerdefinierte Daten verarbeitet und in den Inventarscan eingeschlossen, der an den Core gesendet wird.

Inventarscantypen

XML-Dateien mit benutzerdefinierten Daten, die sich im Verzeichnis "CustomData" befinden, werden im Rahmen eines vollständigen Scans verarbeitet und auch im Rahmen eines Deltascans, der einen Softwarescan umfasst.

Inventarprotokollierung

Der Teil eines Inventarscans, der nach XML-Dateien mit benutzerdefinierten Daten sucht und diese verarbeitet, wird im LANDesk.log als **Idscan : Scanning for custom data** (Nach benutzerdefinierten Daten scannen) aufgezeichnet. Wenn die XML-Dateien mit benutzerdefinierten Daten ordnungsgemäß formatiert sind, erscheinen keine weiteren Einträge bezüglich benutzerdefinierter Daten im Protokoll "LANDesk.log". Tritt jedoch ein Fehler auf, wird dies im LANDesk.log-Protokoll wie folgt dokumentiert: **Idscan: Error opening or loading the CustomData file:filename.xml as XML** (Fehler beim Öffnen oder Laden der CustomData-Datei:Dateiname.xml als XML)

Ein Fehler bei der Verarbeitung einer XML-Datei mit benutzerdefinierten Daten hat nicht zur Folge, dass andere XML-Dateien mit benutzerdefinierten Daten im Verzeichnis für benutzerdefinierte Daten nicht verarbeitet werden. Gleichermaßen führen Fehler bei der Verarbeitung von XML-Dateien mit benutzerdefinierten Daten nicht dazu, dass ein Inventarscan nicht abgeschlossen oder nicht an den Core gesendet werden kann.

Inventar auf dem Core

Im Inventar gespeicherte Informationen über benutzerdefinierten Daten zu einem Gerät, auf dem der LANDesk Agent für Macintosh ausgeführt wird, werden aktualisiert, wenn die XML-Dateien mit benutzerdefinierten Daten, die Informationen enthalten, aktualisiert werden und ein Inventarscan auf dem Client ausgeführt wird, der die benutzerdefinierten Daten aktualisiert.

Denken Sie daran, dass in benutzerdefinierten Daten enthaltene Informationen, die aus den XML-Dateien mit benutzerdefinierten Daten gelöscht werden, nicht aus den Inventardatensätzen auf dem Core entfernt werden. Wenn Sie nicht gewünschte Informationen in benutzerdefinierten Daten aus einem Inventardatensatz auf dem Core entfernen wollen, löschen Sie den Datensatz und senden Sie einen neuen vollständigen Scan von dem Gerät, das durch diesen Datensatz dargestellt wurde.

Fehlerbehebung beim Inventarscanner

In diesem Abschnitt werden allgemeine Probleme des Inventarscanners und mögliche Lösungswege beschrieben.

Der Inventarscanner "hängt"

- Achten Sie darauf, dass die alten /DELL- oder /CPQ-Optionen nicht mit in die Befehlszeile eingegeben werden. Diese Optionen werden nicht mehr unterstützt.
- Scannen Sie eine Datei mithilfe des Parameters /O=. Möglicherweise zeigt dies einen Konflikt mit der Netzwerkkarte oder dem Netzwerk.

Hardware eines Geräts wird korrekt gescannt, die Software jedoch nicht

- Prüfen Sie, ob die Coredatenbank so konfiguriert ist, dass ein Softwarescan sofort ausgeführt wird. Verwenden Sie den Parameter /f, um einen Softwarescan zu erzwingen.
- Scannen Sie eine Datei mithilfe des Parameters /O=. Dadurch sollte die Software am Ende der Datei aufgeführt werden.
- Stellen Sie sicher, dass das Gerät nicht versucht, im CfgFiles-Parameter von LdAppl3.Template in einer Binärdatei zu scannen.

Die Netzwerkansicht enthält nur Inventardaten für einige Geräte

Um Gerätedaten anzuzeigen, müssen Sie sicherstellen, dass die Geräte in die Coredatenbank gescannt wurden. Geräte, die ohne Informationen angezeigt werden, wurden nicht in die Coredatenbank gescannt.

So zeigen Sie die Inventardaten eines Geräts in der Netzwerkansicht an

1. Konfigurieren Sie das Gerät.
2. Scannen Sie das Gerät in die Coredatenbank.

Angeben, wie viele Tage Inventarscans gespeichert werden sollen

Standardmäßig bewahrt der Coreserver Inventarscans so lange auf, bis Sie sie löschen. Sie können den Core anweisen, Geräte-Inventarscans zu löschen, wenn das Gerät während der von Ihnen festgelegten Anzahl von Tagen keinen Scan unterbreitet hat. Auf diese Weise können Sie Geräte entfernen, die sich nicht mehr in Ihrem Netzwerk befinden.

So legen Sie die Anzahl der Dateirevisionen fest, die in der Coredatenbank gespeichert werden soll

1. Klicken Sie auf **Konfigurieren > Dienste > Inventar**.
2. Geben Sie an, wie viele Tage die Inventarscans gespeichert bleiben sollen.
3. Klicken Sie auf **OK**.

Geändertes Vorgehen des Inventarscanners bei der Erfassung von BIOS-Information

Beginnend mit Management Suite 8.7 SP3 verwendet der Inventarscanner nicht mehr den 16-Bit-Inventarscanner zur Erfassung bestimmter BIOS-Daten. Der Scanner meldet standardmäßig nicht mehr die Motherboard-Busnummer, die Geräteattribute des Motherboard-Busses und die Größe angeschlossener Diskettenlaufwerke. Darüber hinaus erstellt der Inventarscanner auf verwalteten Geräten auch keine verborgene LDBIOS.TXT-Datei mit BIOS-Zeichenfolgen mehr.

Wenn Sie veranlassen möchten, dass der Inventarscanner wieder Informationen zu diesen Optionen bereitstellt und die Datei LDBIOS.TXT erstellt, können Sie den Inventarscanner mit dem Schalter /do16 ausführen.

Hilfe zum Inventar

Informationen zum Fenster "Inventar"

Im Fenster **Inventar** können Sie das gesamte Inventar eines Geräts anzeigen, einschließlich folgender Komponenten:

- **BIOS:** Typ, Datum, ID-Byte, Hersteller, ROM-Version, SMBIOS-Version und Systemmodell für das BIOS. Das BIOS befindet sich permanent im ROM (Read-Only Memory, schreibgeschützter Speicher) des Computers und verwaltet die Kommunikation zwischen Speicher, Festplattenlaufwerken und Bildschirm.
  Weitere BIOS-Informationen werden im Fenster "Inventar" als BIOS-Textzeichenfolgen angezeigt. Um BIOS-Textzeichenfolgen anzuzeigen und zu durchsuchen, erweitern Sie das **BIOS**-Objekt, wählen **BIOS-Zeichenfolgen**, klicken mit der rechten Maustaste auf das Attribut **Daten**, wählen **Eigenschaften** und klicken dann auf **Erweiterte Werte**. Während eines Inventarscans werden die verfügbaren Textzeichenfolgen in das BIOS in eine Textdatei mit der Bezeichnung LDBIOS.TXT exportiert. Sie können eine Abfrage in der Datei LdAppl3.ini einrichten, mit der eine oder mehrere der BIOS-Textzeichenfolgen an die Konsole ausgegeben werden. Nähere Informationen finden Sie unter "Hinzufügen von BIOS-Textzeichenfolgen zur Coredatenbank" auf Seite 180.
- **Bus:** Bustyp. Der Bus verbindet den Mikroprozessor, die Festplattenlaufwerke, Speicher und Eingabe-/Ausgabeports miteinander. Es gibt folgende Bustypen: ISA, EISA, VESA Lokaler Bus, PCI und USB.
- **Coprozessor:** Coprozessortyp, sofern vorhanden. Der Coprozessor ist nicht mit dem Hauptmikroprozessor identisch, obwohl er sich auf demselben Motherboard oder sogar demselben Chip befinden kann. Der Math-Coprozessor evaluiert den Gleitkommabetrieb für den Hauptmikroprozessor.
- **Benutzerdefinierte Daten:** Alle vom Benutzer für den Inventarscanner aktivierten Daten.
- **Datenbank:** Datenbanktreiber und Versionsinformationen.
- **Umgebung:** Speicherorte, Befehlspfade, Systemeingabeaufforderungen und andere Variablen für die Windows-Umgebung.
- **Zustand:** Der Gerätezustand, wie er vom LANDesk Agenten festgestellt wurde.

- **Tastatur:** Die an das Gerät angeschlossene Tastatur. Derzeit ist die erweiterte IBM-Tastatur die gebräuchlichste Tastatur. Die Tastatur verwendet Codeseiten.
- **LANDesk Management:** Informationen zu den Agenten, zum Client Manager und Alert Management System (AMS). Enthält auch Informationen zum Inventarscanner und zu den Initialisierungsdateien.
- **Lokale Benutzer und Gruppen:** Die lokalen Windows-Benutzergruppen und Gruppenmitgliedschaften.
- **Massenspeicher:** Speichergeräte auf dem Computer, einschließlich Disketten, Festplatten, logische Laufwerke und Bandlaufwerke sowie CD-ROM. Die Festplatten- und Diskettenlaufwerk-Objekte umfassen Attribute für Kopf, Nummer, Sektor und Gesamtspeicherkapazität.
- **Speicher:** Attribute für Auslagerungsdatei, physischen und virtuellen Speicher. Jedes dieser Speicherobjekte enthält Byte-Attribute. Das erste Byte ist die Größe des verfügbaren Speichers. Das zweite Byte ist die Gesamtspeicherkapazität.
- **Modems**: Die Modeminformationen umfassen den Hersteller, das Modell, die Modellnummer und den Port.
- **Motherboard:** Informationen zum Motherboard, einschließlich Busgeschwindigkeit und Steckplatzinformationen.
- **Maus:** Die an das Gerät angeschlossene Maus. Mögliche Maustypen sind u.a. PS/2, seriell und Infrarot.
- **Multimediadateien:** Anzahl der Dateien mit Erweiterungen, die gängigen Multimediadateitypen entsprechen (.jpg, .mp3 und so weiter) und wie viel Speicherplatz diese benötigen.
- **Netzwerk:** Netzwerkadapter, NIC-Adresse und Knotenadresse der Adapter. Das Netzwerkobjekt enthält Informationen zu jedem Protokoll.
- **Netzwerkadapter:** Attribute für jeden auf dem Gerät installierten Netzwerkadapter.
- **Betriebssystem:** Betriebssystem, Treiber, Dienste und Ports. Diese Objekte und ihre Attribute variieren je nach den Konfigurationen der geladenen Treiber und Dienste.
- **Ports:** Objekte für jeden Ausgabeport des Computers (seriell und parallel). Jeder Ausgabeport enthält Adress- und Namensattribute. Das Adressattribut enthält die Hardwareadresse für den Port.
- **Energieverwaltung:** Die Energieverwaltungseinstellungen auf dem Gerät.
- **Drucker:** Objekte für jeden Drucker, der direkt oder über ein Netzwerk an den Computer angeschlossen ist. Die Druckerobjekte enthalten Treiber-, Namens-, Nummern- und Port-Attribute. Das Port-Attribut enthält entweder die Netzwerkwarteschlange oder den Port, an den der Drucker angeschlossen ist.
- **Prozessor:** Attribute der CPU des Geräts. Erkennt Intel-, Motorola 680x0- und PowerPC-Prozessoren.
- **Ressourcen:** Objekte für alle Hardwareressourcen des Computers. Jedes Objekt einer Hardwareressource enthält Attribute, die den Ressourcentyp und alle von ihm verwendeten Ports und Interrupts beschreiben.
- **Sicherheit:** Antivirus-Software und Version.
- **Software:** Objekte für jede auf der Festplatte des Geräts installierte Softwareanwendung. Jedes Objekt eines Softwareprogramms listet Attribute auf, die typischerweise den Namen, den Speicherort und die Versionsnummer der Software enthalten.
- **System:** Motherboard und Gehäuseinformationen.
- **Systemfähigkeit**: Verschiedene Systemtechnologien wie ASIC-Funktionalität oder Software für virtuelle Computer.
- **ThinkVantage Technologies:** Informationen zu Lenovo ThinkVantage Technologies-Software.

- **Video:** Objekte für jeden Videoadapter des Geräts. Das Videoadapterobjekt enthält im Normalfall Attribute, die die Auflösung und die Anzahl der unterstützten Farben beschreiben.

Informationen zum Dialogfeld "Eigenschaften des Inventarattributs"

In diesem Dialogfeld können Sie die Eigenschaften eines Attributs anzeigen. Die Registerkarte **Merkmale** zeigt folgende Informationen an: Je nach Attribut und abhängig davon, ob Sie ein Attribut hinzufügen, bearbeiten oder anzeigen, sind ggf. nicht alle Felder zu sehen.

- **Name:** Der Name des Coredatenbank-Attributs, dessen Eigenschaften angezeigt werden.
- **Wert:** Der diesem Inventarattribut zugewiesene Wert.
- **Benutzerdefiniert:** Gibt an, ob das ausgewählte Attribut vom Benutzer definiert wurde. Diese Option kann nicht geändert werden.
- **Formatbezeichner (nur Ganzzahlenwerte):** Schreibweise, mit der der Wert in der richtigen Form angezeigt wird. Beispielsweise wird der Attributwert mit "%d MB" ohne Dezimalstellen angezeigt; mit "%.1f MB" wird der Attributwert bis zur ersten Gleitkommastelle in MB angezeigt. Wenn kein Faktor eingegeben wird, muss dieser Formatbezeichner Ganzzahlenwerte beschreiben (%d, %u usw.). Wenn ein Faktor eingegeben wird, muss dieser Formatbezeichner Gleitkommawerte beschreiben (%f).
- **Faktor (nur Ganzzahlenwerte):** Ganzzahlenwerte, mit denen das Attribut in Einheiten unterteilt wird. Wenn Sie den Faktorwert ändern, müssen Sie den entsprechenden Code im Feld "Formatbezeichner" eingeben. Wenn das Attribut in Kilobyte angegeben wurde und jetzt in Megabyte angezeigt werden soll, geben Sie den Wert "1000" ein.
- **Formatierter Wert:** Beispieltext für das angegebene Format und den angegebenen Faktor.

Informationen zum Dialogfeld "Inventaränderungseinstellungen"

Verwenden Sie dieses Dialogfeld, um auszuwählen, welche Inventarattribute protokolliert werden, wenn Änderungen an einzelnen Geräten vorgenommen werden, und um anzugeben, wo diese Änderungen protokolliert werden.

- **Aktuelles Inventar:** Listet alle in der Coredatenbank gespeicherten Objekte auf. Klicken Sie auf ein Objekt, um dessen Attribute in der Liste **Ereignis protokollieren in** anzuzeigen. Erweitern Sie eine Objektgruppe, um die darin enthaltenen Datenobjekte anzuzeigen.
- **Ereignis protokollieren in:** Zeigt die Attribute des in der Liste **Aktuelles Inventar** ausgewählten Inventarobjekts an.
  Um festzulegen, wo Inventaränderungen protokolliert werden, wählen Sie ein Attribut aus und aktivieren eine oder mehrere Optionen. Wählen Sie die Option **Inventar** aus, um Inventaränderungen im Dialogfeld **Inventaränderungsverlauf** des Geräts zu protokollieren. Wählen Sie die Option **NT-Protokoll** aus, um Inventaränderungen im Windows NT-Ereignisprotokoll zu erfassen. Wählen Sie die Option **AMS** aus, um Inventaränderungen als Alarm über AMS zu senden. (Konfigurieren Sie AMS-Alarmmeldungen mit dem Tool "Alarmeinstellungen".)
- **Protokoll/Alarmwichtigkeit:** Enthält die Optionen für die Alarmpriorität. Diese Funktion wird erst aktiviert, wenn ein Attribut ausgewählt ist. Sie können zwischen den Prioritätsstufen "Keine", "Informationen", "Warnung" und "Kritisch" wählen.

Informationen zum Dialogfeld "Inventaränderungsverlauf"

In diesem Dialogfeld können Sie die Inventaränderungen eines Geräts anzeigen. Außerdem können Sie den Inventaränderungsverlauf über dieses Dialogfeld drucken und exportieren.

- **Gerätename:** Zeigt den Namen der Geräte an, die in der Netzwerkansicht der Konsole ausgewählt wurden und für die Inventaränderungsdaten angefordert wurden.

- **Komponente:** Gibt die geänderte Systemkomponente an. (Hier werden nur Komponenten angezeigt, die im Dialogfeld **Inventaränderungseinstellungen** ausgewählt wurden.)
- **Attribut:** Gibt an, welches Attribut der Komponente protokolliert wird.
- **Zeit:** Gibt an, wann die Änderung erfolgt ist.
- **Neuer Wert:** Zeigt den neuen (geänderten) Wert für das angegebene Attribut.
- **Alter Wert:** Zeigt den alten (vorherigen) Wert für das angegebene Attribut.
- **Drucken:** Öffnet ein Standarddialogfeld zum Drucken, mit dem Sie den Inhalt des Inventaränderungsverlaufs drucken können.
- **Exportieren:** Öffnet das Dialogfeld "Speichern unter", in dem Sie einen Namen und den Speicherort der exportieren .CSV-Datei mit dem Inventaränderungsverlauf auswählen können.

HINWEIS: Im Dialogfeld **Inventaränderungsverlauf** wird der Verlauf in chronologischer Ordnung angezeigt. Sie können diese Daten nicht sortieren, indem Sie auf die Spaltenüberschrift klicken.

Informationen zum Dialogfeld "Benutzerdefiniertes Datenformular erstellen/bearbeiten"

Benutzerdefinierte Datenformulare werden in LANDesk Security Suite nicht unterstützt. Benutzerdefinierte Datenformulare stehen bei einer reinen LANDesk Security Suite Lizenz nicht zur Verfügung. Sie müssen im Besitz einer LANDesk Management Suite Volllizenz sein, um die Funktion "Benutzerdefinierte Formulare" verwenden zu können.

In diesem Dialogfeld können Sie ein benutzerdefiniertes Datenformular erstellen oder bearbeiten.

- **Formularname:** Identifiziert das Formular und ist auf der Formularanzeige zu sehen, wenn ein Benutzer das Formular ausfüllt.
- **Beschreibung:** Stellt Benutzern zusätzliche Informationen zum Formular zur Verfügung.
- **Hinzufügen:** Öffnet das Dialogfeld **Frage hinzufügen**, in dem Sie eine neue Frage für das Formular erstellen können.
- **Bearbeiten:** Öffnet das Dialogfeld **Frage bearbeiten**, in dem Sie die Optionen einer beliebigen Frage bearbeiten können.
- **Löschen:** Löscht die Frage aus dem Formular.
- **Seitenumbruch:** Steuert das Layout des Formulars, indem Seitenumbrüche zwischen zusammengehörigen Fragengruppen eingefügt werden. Bei einem Seitenumbruch müssen Benutzer auf "Weiter" klicken, um zu den Fragen auf der nächsten Seite zu gelangen.

HINWEIS: Pro Seite werden maximal neun Fragen unterstützt.

- **Vorschau:** Öffnet das Formular, damit Sie vorab sehen können, wie das Formular für Benutzer angezeigt wird. Im Vorschaumodus müssen Sie keine Daten einfügen und Ihre Eingaben werden nicht gespeichert.

Informationen zum Dialogfeld "Frage hinzufügen/bearbeiten"

In diesem Dialogfeld können Sie Fragen erstellen oder bearbeiten, die auf dem benutzerdefinierten Datenformular angezeigt werden. Formulare bestehen aus Fragen und freiem Platz, in dem Benutzer ihre Antworten eingeben können. Legen Sie zunächst die Frage fest:

- **Fragetext:** Einzeilige Beschreibung der Frage. Dieser Text wird neben dem Datenfeld angezeigt.
- **Inventarname:** Name des Datenbankfeldes in der Coredatenbank. Wenn Sie die Coredatenbank nach diesem Element abfragen möchten, erstellen Sie eine Abfrage nach der Beschriftungskennung.
- **Beschreibung:** Zusätzliche Angaben, die angezeigt werden, wenn Benutzer auf **Hilfe** klicken (oder die **F1**-Taste drücken, während sich der Cursor im Datenfeld dieser Frage befindet).

Sie müssen auch angeben, welche Art von Datenfeld (Steuerung) neben jeder Frage angezeigt wird und ob es ein erforderliches Feld ist. Folgende Datenfelder stehen zur Verfügung:

- **Bearbeitungsfeld:** Benutzer geben ihre Antwort in ein editierbares Textfeld ein.
- **Kombinationsfeld (Bearbeitungsliste):** Benutzer wählen einen der vordefinierten Listeneinträge aus oder geben eine eigene Antwort ein.
- **Kombinationsfeld (feste Liste):** Benutzer wählen einen der vordefinierten Listeneinträge aus.
- **Steuerung ist erforderliches Feld und muss ausgefüllt werden:** Der Benutzer ist gezwungen, diese Frage zu beantworten. Der Benutzer kann das Formular erst beenden oder zur nächsten Seite wechseln, wenn er eine Antwort in die erforderlichen Felder eingegeben hat.

Informationen zum Dialogfeld "Elemente hinzufügen"

Verwenden Sie dieses Dialogfeld, um Elemente in eine Dropdownliste einzufügen, aus der ein Benutzer Antworten für diese Frage auf einem Formular auswählen kann.

- **Elementname:** Identifiziert das Element. Dieser Name wird in der Liste der Frage angezeigt.
- **Elementliste:** Enthält alle Elemente, die in der Liste der Frage angezeigt werden.
- **Einfügen:** Fügt das Element in die Elementliste ein.
- **Löschen:** Löscht das Element aus der Elementliste.

Informationen zum Dialogfeld "Mehrere Formulare zur Verteilung auswählen"

In diesem Dialogfeld erstellen Sie eine Gruppe von Formularen. Es zeigt den Namen der Gruppe und alle verfügbaren Formulare, die Teil einer Gruppe sein können.

- **Name der neuen Gruppe:** Identifiziert die Gruppe im Fenster **Benutzerdefinierte Datenformulare**.
- **Verfügbare Formulare:** Zeigt alle verfügbaren Formulare an, die zu dieser Gruppe hinzugefügt werden können.
- **OK:** Speichert die Gruppe und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Gruppe zu speichern.

Abfragen/Verzeichnis-Manager

Datenbankabfragen

Abfragen sind benutzerdefinierte Suchvorgänge nach verwalteten Geräten. LANDesk Management Suite stellt eine Methode zur Verfügung, mit der Sie Abfragen für Geräte, die mittels Datenbankabfragen in Ihre Coredatenbank gescannt wurden, erstellen können. In LANDesk Management Suite ebenfalls verfügbar ist eine Methode, mit der Sie über LDAP-Abfragen nach Geräten in anderen Verzeichnissen suchen können. Mit der Gruppe "Abfragen" können Sie Datenbankabfragen in der Netzwerkansicht der Konsole anzeigen, erstellen und ordnen.

Mithilfe von Abfragen können Sie auf der Basis bestimmter System- oder Benutzerkriterien nach in der Coredatenbank gespeicherten Netzwerkgeräten suchen und diese entsprechend ordnen. Damit steht Ihnen ein praktisches Hilfsmittel für die Netzwerkverwaltung zur Verfügung.

So können Sie beispielsweise eine Abfrage erstellen und ausführen, die nur Geräte mit einer Taktgeschwindigkeit von weniger als 2 GHz, weniger als 1024 MB Arbeitsspeicher oder einer Festplatte mit weniger als 20 GB Speicherkapazität erfasst. Erstellen Sie eine oder mehrere Abfrageanweisungen für diese Bedingungen und verknüpfen Sie diese Anweisungen mithilfe von logischen Operatoren. Wenn die Abfragen ausgeführt wurden, können Sie die Ergebnisse drucken, auf die entsprechenden Geräte zugreifen und sie verwalten.

Abfragegruppen

Abfragen können in der Netzwerkansicht in Gruppen organisiert werden. Erstellen Sie neue Abfragen (und neue Abfragegruppen), indem Sie mit der rechten Maustaste entweder auf die Gruppe **Eigene Abfragen** klicken oder **Neue Abfrage** bzw. **Neue Gruppe** auswählen.

Ein Management Suite Administrator (Benutzer mit Management Suite Administratorrechten) kann den Inhalt aller Abfragegruppen anzeigen. Dazu gehören: **Eigene Abfragen**, **Öffentliche Abfragen** und **Alle Abfragen.**

Andere Management Suite Benutzer, die sich bei der Konsole anmelden, können (abhängig von ihrem Gerätebereich) die Gruppen **Eigene Abfragen**, **Öffentliche Abfragen** und **Alle Abfragen** sehen.

Wenn Sie eine Abfrage in eine Gruppe verschieben (durch Klicken mit der rechten Maustaste und Auswählen von **Zu neuer Gruppe hinzufügen** oder **Zur vorhandenen Gruppe hinzufügen** bzw. durch Ziehen und Ablegen der Abfrage), erstellen Sie eine Kopie der Abfrage. Sie können die Kopie in jeder Abfragegruppe entfernen – die Masterkopie der Abfrage (in der Gruppe **Alle Abfragen**) bleibt davon unberührt. Die Masterkopie kann von der Gruppe **Alle Abfragen** aus gelöscht werden.

Erstellen einer Datenbankabfrage

Verwenden Sie das Dialogfeld **Neue Abfrage**, um eine Abfrage durch Auswählen von Attributen, relationalen Operatoren und Attributwerten zu erstellen. Erstellen Sie eine Abfrageanweisung, indem Sie ein Inventarattribut auswählen und es mit einem akzeptablen Wert verknüpfen. Verknüpfen Sie die Abfrageanweisungen logisch miteinander, um sicherzustellen, dass sie als Gruppe ausgewertet werden, bevor Sie sie mit anderen Anweisungen oder Gruppen verknüpfen.

So erstellen Sie eine Datenbankabfrage

1. Klicken Sie in der Netzwerkansicht der Konsole mit der rechten Maustaste auf die Gruppe Eigene Abfragen (oder **Öffentliche Abfragen**, wenn Sie das entsprechende Recht zur Verwaltung öffentlicher Abfragen besitzen) und klicken Sie dann auf **Neue Abfrage**.
2. Geben Sie einen eindeutigen Namen für die Abfrage ein.
3. Wählen Sie eine Komponente aus der Inventarattributliste aus.
4. Wählen Sie einen relationalen Operator aus.
5. Wählen Sie einen Wert aus der Werteliste. Sie können den Wert bearbeiten.
6. Klicken Sie auf **Einfügen**, um die Anweisung zur Abfrageliste hinzuzufügen.
7. Wenn Sie eine Abfrage für mehrere Komponenten ausführen möchten, klicken Sie auf einen **logischen Operatoren (AND, OR)** und wiederholen Sie die Schritte 2 bis 5.
8. (Optional) Um Abfrageanweisungen so zu gruppieren, dass sie als Gruppe ausgewertet werden, wählen Sie zwei oder mehrere **Abfrageanweisungen** und klicken auf **Gruppieren ( )**.
9. Wenn Sie alle Anweisungen hinzugefügt haben, klicken Sie auf **Speichern**.

Ausführen einer Datenbankabfrage

So führen Sie eine Abfrage aus

1. Erweitern Sie in der Netzwerkansicht die Abfragegruppen, damit Sie die auszuführende Abfrage suchen können.
2. Doppelklicken Sie auf die Abfrage. Alternativ dazu können Sie auch mit der rechten Maustaste klicken und **Ausführen** wählen.
3. Die Ergebnisse (passenden Geräte) werden im rechten Fensterbereich der Netzwerkansicht angezeigt.

Importieren und Exportieren von Abfragen

Sie können über die Import- und Exportfunktionen Abfragen aus einer Coredatenbank in eine andere übertragen. Sie können Folgendes importieren:

- exportierte Abfragen aus Management Suite 8 und 9 sowie
- mit der Webkonsole exportierte .XML-Abfragen.

So importieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die Abfragegruppe, in welche die Abfrage importiert werden soll.
2. Wählen Sie **Importieren** aus dem Kontextmenü.
3. Navigieren Sie zur Abfrage, die Sie importieren möchten, und wählen Sie sie aus.
4. Klicken Sie auf **Öffnen**, um die Abfrage zur ausgewählten Abfragegruppe in der Netzwerkansicht hinzuzufügen.

So exportieren Sie eine Abfrage

1. Klicken Sie mit der rechten Maustaste auf die zu exportierende Abfrage.
2. Wählen Sie **Exportieren** aus dem Kontextmenü.

3. Navigieren Sie zu dem Verzeichnis, in dem Sie die Abfrage (als .ldms-Datei) speichern möchten.
4. Geben Sie einen Namen für die Abfrage ein.
5. Klicken Sie auf **Speichern**, um die Abfrage zu exportieren.

LDAP-Abfragen

Management Suite bietet neben der Möglichkeit zur Abfrage der Coredatenbank auch die Möglichkeit, mit dem Extra "Verzeichnis-Manager" über LDAP (Lightweight Directory Access Protocol) nach Geräten in anderen Verzeichnissen zu suchen und auf diese Geräte zuzugreifen und sie zu verwalten.

Sie können Geräte auch auf der Basis von Attributen wie Prozessortyp oder Betriebssystem abfragen. Die Abfrage kann auch auf bestimmten Benutzerattributen wie Personalnummer oder Abteilung basieren.

Weitere Informationen zum Erstellen und Ausführen von Datenbankabfragen aus der Gruppe "Abfragen" in der Netzwerkansicht finden Sie unter "Abfragen/Verzeichnis-Manager" auf Seite 193.

LDAP-Verzeichnisse konfigurieren

Verwenden Sie das Extra "Verzeichnis-Manager" zur Verwaltung der LDAP-Verzeichnisse, die Sie mit LANDesk Management Suite nutzen. Ihr eingegebener LDAP-Server, Benutzername und das Kennwort werden gespeichert und verwendet, wenn Sie Abfragen ans Verzeichnis durchsuchen oder ausführen. Wenn Sie das Kennwort des konfigurierten Benutzers im LDAP-Verzeichnis ändern, müssen Sie es auch in diesem Extra ändern.

HINWEIS: Das im Verzeichnis-Manager konfigurierte Konto muss die Benutzer, Computer und Gruppen lesen können, die Sie zur Verwaltung mit LDMS verwenden.

So konfigurieren Sie ein neues Verzeichnis

1. Klicken Sie auf **Konfigurieren > Verzeichnisse verwalten**.
2. Klicken Sie auf **Hinzufügen**.
3. Geben Sie den DNS-Namen des Verzeichnisservers im Feld **LDAP://** an.
4. Geben Sie den **Benutzernamen** und das **Kennwort** ein.

HINWEIS: Wenn Sie Active Directory verwenden, geben Sie den Namen als <domain-name>\<nt-user-name> ein. Wenn Sie einen anderen Verzeichnisdienst verwenden, geben Sie den eindeutigen Namen des Benutzers ein.

5. Klicken Sie auf **OK**, um die Informationen zu speichern. Die von Ihnen eingegebenen Informationen werden gegen das Verzeichnis geprüft, bevor das Dialogfeld geschlossen wird.

So ändern Sie eine bestehende Verzeichniskonfiguration

1. Klicken Sie auf **Konfigurieren > Verzeichnisse verwalten**.
2. Klicken Sie auf das gewünschte Verzeichnis.
3. Klicken Sie auf **Bearbeiten**.
4. Ändern Sie je nach Wunsch den Server, Benutzernamen oder das Kennwort.

5. Klicken Sie auf **OK**, um die Informationen zu speichern. Die Informationen werden gegen das Verzeichnis geprüft, bevor das Dialogfeld geschlossen wird.

So löschen Sie eine bestehende Verzeichniskonfiguration

1. Klicken Sie auf **Konfigurieren > Verzeichnisse verwalten**.
2. Klicken Sie auf das gewünschte Verzeichnis.
3. Klicken Sie auf **Löschen**.

HINWEIS: Alle LDAP-Abfragen, die dieses Verzeichnis verwenden, werden gelöscht, wenn dieses Verzeichnis entfernt wird.

Erstellen einer LDAP-Verzeichnisabfrage

Die Aufgabe der Erstellung einer Verzeichnisabfrage und des Speicherns dieser Abfrage gliedert sich in zwei Schritte:

So wählen Sie ein Objekt im LDAP-Verzeichnis aus und initiieren eine neue Abfrage

1. Klicken Sie auf **Extras > Verteilung > Verzeichnis-Manager**.
2. Durchsuchen Sie den Verzeichnisbereich **Verzeichnis-Manager** und wählen Sie ein Objekt im LDAP-Verzeichnis aus. Sie erstellen damit eine LDAP-Abfrage, die Ergebnisse von diesem Punkt ausgehend nach unten im Verzeichnisbaum ausgibt.
3. Klicken Sie vom Verzeichnis-Manager aus in der Symbolleiste auf die Schaltfläche **Neue Abfrage**. Beachten Sie, dass dieses Symbol nur angezeigt wird, wenn Sie die Stammorganisation (o) des Verzeichnisbaums (o=mein Unternehmen) oder eine Organisationseinheit (ou=Engineering) innerhalb der Stammorganisation auswählen. Andernfalls ist es ausgeblendet.
4. Das Dialogfeld **Einfache LDAP-Abfrage** wird angezeigt.

So erstellen, testen und speichern Sie die Abfrage

1. Klicken Sie im Dialogfeld **Einfache LDAP-Abfrage** auf ein Attribut, das ein Kriterium für die Abfrage aus der Liste der Verzeichnisattribute sein soll (Beispiel = Abteilung).
2. Klicken Sie auf einen Vergleichsoperator für die Abfrage (=,<=, >=).
3. Geben Sie einen Wert für das Attribut ein (Beispiel Abteilung = Engineering).
4. Um eine komplexe Abfrage mit mehreren Attributen zu erstellen, wählen Sie einen Kombinationsoperator (AND oder OR) und wiederholen Schritte 1 bis 3 so oft wie nötig.
5. Wenn Sie die Erstellung der Abfrage beendet haben, klicken Sie auf **Einfügen**.
6. Zum Testen der fertig gestellten Abfrage klicken Sie auf **Abfrage testen**.
7. Zum Speichern der Abfrage klicken Sie auf **Speichern**. Die gespeicherte Abfrage erscheint mit ihrem Namen unter **Gespeicherte Abfragen** im Verzeichnisbereich des Verzeichnis-Managers.

Informationen zum Verzeichnis-Manager-Fenster

Mit dem Verzeichnis-Manager können Sie folgende Aufgaben ausführen:

- **Verzeichnis verwalten:** Öffnet das Dialogfeld **Verzeichniseigenschaften**. In diesem Dialogfeld können Sie ein LDAP-Verzeichnis identifizieren und sich bei einem solchen Verzeichnis anmelden.

- **Verzeichnis entfernen:** Entfernt das ausgewählte Verzeichnis aus dem vorherigen Fensterausschnitt und stellt die Verwaltung ein.
- **Ansicht aktualisieren:** Lädt die Liste der verwalteten Verzeichnisse und Zielbenutzer neu.
- Organisationsansicht starten:
- **Neue Abfrage:** Öffnet das Dialogfeld **LDAP-Abfrage**, in dem Sie eine LDAP-Abfrage erstellen und speichern können.
- **Abfrage löschen:** Löscht die ausgewählte Abfrage.
- **Abfrage ausführen:** Erzeugt die Ergebnisse der ausgewählten Abfrage.
- **Objekteigenschaften:** Zeigt die Eigenschaften des ausgewählten Objekts.

Mithilfe des Verzeichnis-Managers können Sie LDAP-Gruppen und gespeicherte LDAP-Abfragen auf geplante Tasks ziehen und sie auf diese Weise als Taskziele ansprechen.

Das Fenster "Verzeichnis-Manager" ist in zwei Bereiche unterteilt: einen Verzeichnisbereich links und einen Vorschaubereich rechts.

Verzeichnisbereich

Der Verzeichnisbereich zeigt alle registrierten Verzeichnisse und Benutzer. Als Administrator können Sie den Namen eines registrierten Verzeichnisses angeben und erhalten eine Liste der Abfragen, die mit diesem Verzeichnis verknüpft sind. Sie können mithilfe eines Rechtsklicks oder der Dropdown-Menüs neue Abfragen für ein registriertes Verzeichnis erstellen und speichern. Nachdem Sie eine Abfrage erstellt haben, können Sie diese mit Ziehen und Ablegen in das Fenster **Geplante Tasks** verschieben, sodass der Task auf Benutzer angewendet wird, die die Bedingungen der Abfrage erfüllen.

Vorschaubereich

Wenn Sie eine gespeicherte Abfrage im Verzeichnisbereich des Verzeichnis-Managers auf der linken Seite des Dialogfelds auswählen, werden die für diese Abfrage bestimmten Richtlinien und Tasks im Vorschaubereich auf der rechten Seite angezeigt. Wenn ein einzelner LDAP-Benutzer im Verzeichnisbereich ausgewählt wird, werden die Richtlinien und Tasks, die für diesen Benutzer bestimmt sind, im Vorschaubereich angezeigt.

Informationen zum Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) ist ein dem Industriestandard entsprechendes Protokoll für den Zugriff auf und die Anzeige von Informationen über Benutzer und Geräte. LDAP ermöglicht Ihnen die Organisation und Speicherung dieser Informationen in einem Verzeichnis. Ein LDAP-Verzeichnis ist insofern dynamisch, als dass es ggf. aktualisiert werden kann. Es wird verteilt, wodurch ein Schutz vor einem zentralen Ausfall gegeben ist. Zu allgemeinen LDAP-Verzeichnissen gehören Novell Directory Services (NDS) und Microsoft Active Directory Services (ADS).

Die nachstehenden Beispiele beschreiben LDAP-Abfragen, die zum Durchsuchen des Verzeichnisses verwendet werden können:

- Alle Einträge abrufen: (objectClass=*)
- Einträge abrufen, die 'bob' an irgendeiner Stelle des Namens enthalten: (cn=*bob*)
- Einträge mit einem allgemeinen Namen abrufen, die größer/gleich 'bob' sind: (cn>='bob')
- Alle Benutzer mit einem E-Mail-Attribut abrufen: (&(objectClass=user)(email=*))

- Alle Benutzereinträge mit einem E-Mail-Attribut und einem Nachnamen abrufen, der 'smith' entspricht: (&(sn=smith)(objectClass=user)(email=*))
- Alle Benutzereinträge mit einem Namen abrufen, der mit 'andy', 'steve' oder 'margaret' beginnt: (& (objectClass=User) (| (cn=andy*)(cn=steve*)(cn=margaret*)))
- Alle Benutzer ohne E-Mail-Attribut abrufen: (!(email=*))

Die formale Definition des Suchfilters ist wie folgt (von RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> > <or> > <not> > <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> > <filter> <filterlist>
- <item> ::= <simple> > <present> > <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> > <approx> > <ge> > <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL > <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL > <value> '*' <starval>
- <final> ::= NULL > <value>

Das Token <attr> ist eine Zeichenfolge, die einen Attributtyp repräsentiert. Das Token <value> ist eine Zeichenfolge, die einen Attributwert repräsentiert, dessen Format vom zugrunde liegenden Verzeichnisdienst definiert wird.

Wenn ein <value> eines der folgenden Zeichen * oder (or) enthalten muss, stellen Sie den Backslash (\) vor das Zeichen.

Informationen zum Dialogfeld "Einfache LDAP-Abfrage"

- **LDAP-Abfragestamm:** Wählen Sie ein Stammobjekt im Verzeichnis für diese Abfrage (LDAP://ldap.xyzunternehmen.com/ou = Amerika.o = xyzunternehmen). Die von Ihnen erstellte Abfrage gibt von diesem Punkt ausgehend nach unten im Baum Ergebnisse aus.
- **LDAP-Attribute:** Wählen Sie Attribute für Benutzertyp-Objekte aus.
- **Operator:** Wählen Sie die Art des auszuführenden Vorgangs in Bezug auf ein LDAP-Objekt, dessen Attribute und Attributwerte einschließlich ist gleich (=), kleiner/gleich (<=) und größer/gleich (>=).
- **Wert:** Geben Sie den Wert an, der dem Attribut eine LDAP-Objekts zugewiesen wurde.
- **AND/OR/NOT:** Boolesche Operatoren, die Sie für Ihre Abfragebedingungen auswählen können.
- **Abfrage testen:** Testen Sie die von Ihnen erstellte Abfrage.

- **Speichern:** Speichern Sie die erstellte Abfrage unter ihrem Namen.
- **Erweitert:** Erstellen Sie eine Abfrage unter Verwendung der Elemente einer einfachen LDAP-Abfrage, jedoch in einem freien Format.
- **Einfügen:** Fügen Sie eine Zeile mit Abfragekriterien ein.
- **Löschen:** Löschen Sie eine ausgewählte Zeile mit Kriterien.
- **Alle löschen:** Löschen Sie alle Zeilen der Abfragekriterien.

Informationen zum Dialogfeld "Erweiterte LDAP-Abfrage"

Klicken Sie im Dialogfeld **Einfache LDAP-Abfrage** auf **Erweitert**, um das Dialogfeld **Erweiterte LDAP-Abfrage** zu öffnen, das folgende Optionen beinhaltet:

- **LDAP-Abfragestamm:** Hiermit können Sie ein Stammobjekt im Verzeichnis für diese Abfrage auswählen. Die von Ihnen erstellte Abfrage gibt von diesem Punkt ausgehend nach unten im Baum Ergebnisse aus.
- **LDAP-Abfrage:** Hiermit können Sie eine Abfrage unter Verwendung der Elemente einer einfachen LDAP-Abfrage erstellen, jedoch in einem freien Format.
- **Beispiele:** Zeigt Abfragebeispiele an, an denen Sie sich beim Erstellen Ihrer eigenen Abfrage (freies Format) orientieren können.
- **Abfrage testen:** Hiermit können Sie die Abfrage testen, die Sie erstellt haben.

Das Dialogfeld **Erweiterte LDAP-Abfrage** wird angezeigt, wenn Sie eine bereits erstellte Abfrage bearbeiten. Wenn Sie eine LDAP-Gruppe im Verzeichnis-Manager auswählen und mit dieser Gruppe als Ausgangspunkt eine Abfrage erstellen, wird das Dialogfeld **Erweiterte LDAP-Abfrage** mit einer Standardabfrage angezeigt, die die Benutzer zurückgibt, die dieser Gruppe angehören. Sie können die Syntax dieser Standardabfrage nicht ändern, sondern lediglich die Abfrage speichern.

Informationen zum Dialogfeld "Active Directory-Quelle"

Klicken Sie in der Verzeichnis-Manager-Symbolleiste auf die Schaltfläche **Verzeichnis verwalten**, um das Dialogfeld **Active Directory-Quelle** zu öffnen. Dieses Dialogfeld ermöglicht Ihnen die Verwaltung eines neuen Verzeichnisses oder die Anzeige der Eigenschaften eines derzeit verwalteten Verzeichnisses. Dieses Dialogfeld zeigt auch die URL zum LDAP-Server und die Authentifizierungsdaten, die für die Verbindung mit dem LDAP-Verzeichnis erforderlich sind.

- **Verzeichnispfad:** Hiermit können Sie das zu verwaltende LDAP-Verzeichnis angeben. Beispiel eines LDAP-Verzeichnisses mit korrekter Syntax: ldap.<Unternehmensname>.com. Sie können beispielsweise ldap.xyzunternehmen.com eingeben.
- **Authentifizierung:** Gibt Ihnen die Möglichkeit, sich als folgender Benutzer anzumelden (d. h., Sie geben einen Benutzerpfad, einen Namen und ein Benutzerkennwort an).

Informationen zum Dialogfeld "LDAP-Abfrage speichern"

Klicken Sie im Dialogfeld **Einfache LDAP-Abfrage** auf **Speichern**, um das Dialogfeld **LDAP-Abfrage speichern** zu öffnen, das folgende Optionen umfasst:

- **Einen Namen für diese Abfrage wählen:** Gibt Ihnen die Möglichkeit, einen Namen für die von Ihnen erstellte Abfrage auszuwählen.

- **Abfragedetails: LDAP-Stamm:** Hiermit können Sie eine Abfrage unter Verwendung der Elemente einer einfachen LDAP-Abfrage erstellen, jedoch in einem freien Format.
- **Abfragedetails: LDAP-Abfrage:** Zeigt Abfragebeispiele an, an denen Sie sich beim Erstellen Ihrer eigenen Abfrage (freies Format) orientieren können.
- **Speichern:** Gibt Ihnen die Möglichkeit, die erstellte Abfrage unter ihrem Namen zu speichern. Die Abfrage wird unter dem Objekt **Gespeicherte Abfragen** des LDAP-Verzeichniseintrags im Verzeichnisbereich des Verzeichnis-Managers gespeichert.

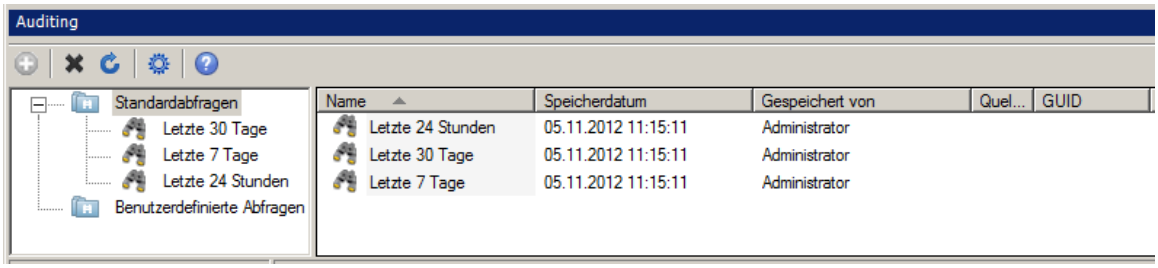
Auditing

Willkommen beim Auditing

Das Extra "Auditing" überwacht die Aktivitäten der Konsolenbenutzer und speichert die Auditingdaten in der Coredatenbank sowie optional im Windows-Ereignisprotokoll.

Das Extra "Auditing" ist standardmäßig nicht aktiviert oder sichtbar. Bevor Sie die Auditingfunktion verwenden können, müssen Sie einem Benutzer Rechte für die Überwachungskonfiguration erteilen und anschließend konfigurieren, welche Aktivitäten überwacht werden sollen.

Wurde Auditing nicht konfiguriert, werden lediglich Änderungen bei der Überwachungskonfiguration überwacht, beispielsweise das Erteilen oder Entfernen von Auditingrechten.



Nähere Informationen hierzu finden Sie in den folgenden Themen:

- "Konfigurieren des Extras "Auditing"" auf Seite 201
- "Senden von Überwachungsereignissen an die Windows-Ereignisanzeige" auf Seite 204
- "Anzeigen von Überwachungsereignissen" auf Seite 206
- "Erstellen von Filtern für Überwachungsereignisabfragen" auf Seite 207

Konfigurieren des Extras "Auditing"

Das Extra "Auditing" ist standardmäßig nicht aktiviert oder sichtbar. Sie können das Extra "Auditing" nur dann anzeigen oder Änderungen an der Überwachungskonfiguration vornehmen, wenn Ihnen von einem Administrator die Rolle "Auditor" oder die Rolle "Überwachungskonfiguration" zugewiesen wurde.

Es gibt zwei Auditingrollen:

- **Überwachungskonfiguration:** Benutzer, denen diese Rolle zugeteilt wurde, können konfigurieren, was überwacht werden soll. Diese Rolle umfasst zudem die Rechte der Rolle "Auditor", d. h. Benutzer, denen diese Rolle zugeteilt wurde, können das Extra "Auditing" anzeigen und Auditingaten einsehen.
- **Auditor:** Benutzer, denen diese Rolle zugeteilt wurde, können Auditingdaten anzeigen und benutzerdefinierten Auditabfragen erstellen, aber nicht ändern, was überprüft wird.

Die Konfiguration des Auditings umfasst drei wesentliche Schritte:

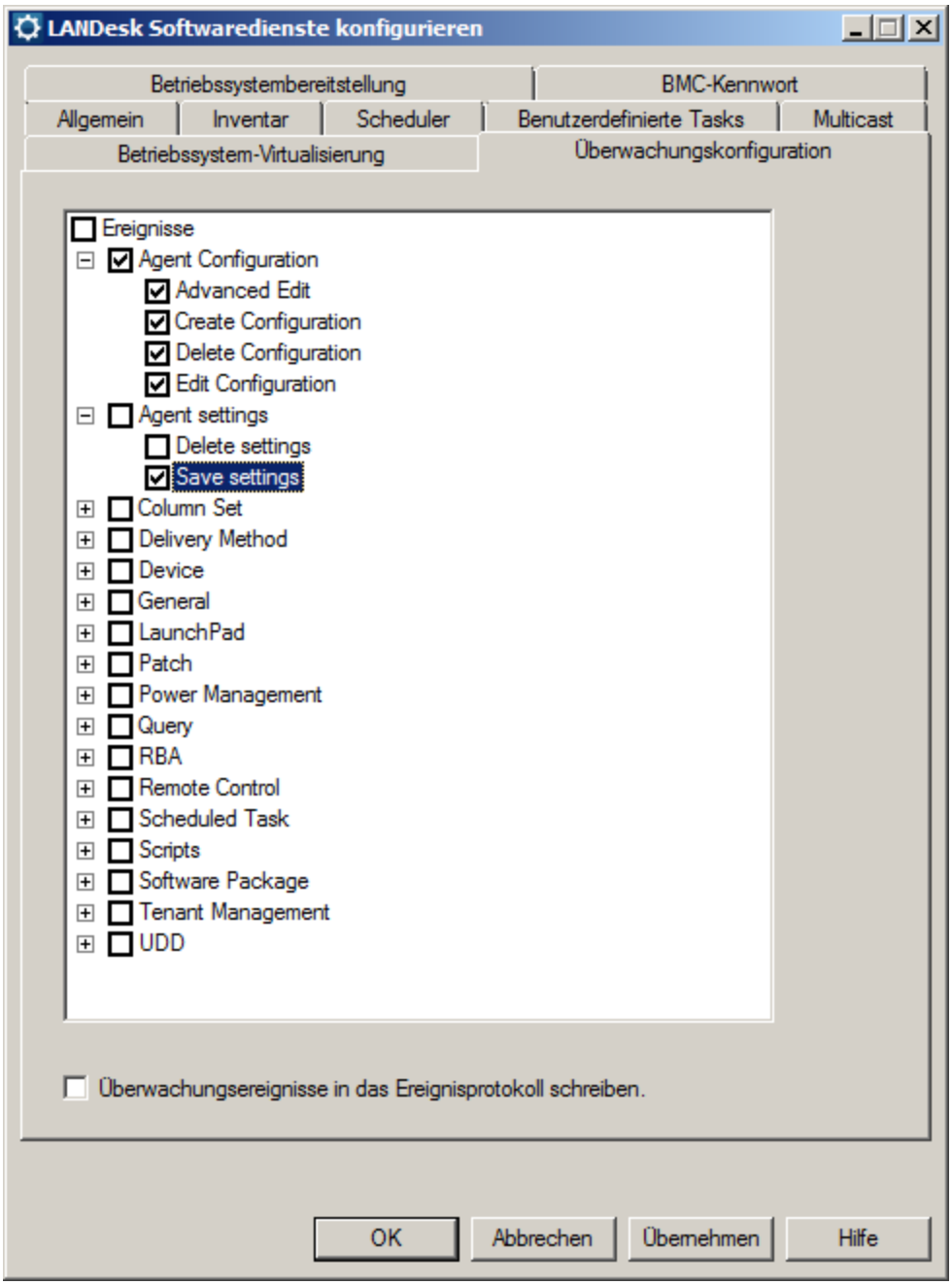
1. Einem Benutzer die Rolle "Überwachungskonfiguration" zuweisen
2. Konfigurieren, was überwacht wird
3. Zusätzlichen Benutzern die Rolle "Auditor" zuweisen, falls erforderlich

So weisen Sie einem Benutzer die Rolle "Überwachungskonfiguration" zu

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie im Baum **Rollen** doppelt auf **Überwachungskonfiguration**.
3. Wählen Sie auf der Seite **Benutzer und Gruppen** die Benutzer aus, denen die Rolle "Überwachungskonfiguration" zugewiesen werden soll.
4. Klicken Sie auf **OK**.
5. Veranlassen Sie die Benutzer, denen Sie die Rolle "Überwachungskonfiguration" zugewiesen haben, ihre Konsole neu zu starten, damit sie das Extra "Auditing" sehen können. Die Rechte und Rollen eines Benutzers, werden nur einmal beim Konsolenstart geladen, daher muss die Konsole neu gestartet werden.

So konfigurieren Sie, was überwacht werden soll

1. Klicken Sie auf **Extras > Dienste konfigurieren**.
2. Klicken Sie im Dialogfeld **LANDesk Softwaredienste konfigurieren** auf die Registerkarte **Überwachungskonfiguration**. Falls diese Registerkarte nicht angezeigt wird, stellen Sie sicher, dass Ihnen die Rolle "Überwachungskonfiguration" zugewiesen wurde und Sie die Konsole im Anschluss an die Zuweisung dieser Rolle neu gestartet haben.



3. Wählen Sie die Konsolenfunktionen oder ungeordneten Funktionen aus, die Sie überwachen wollen.

4. Klicken Sie auf **OK**.
5. Klicken Sie auf **Extras > Administration > Auditing**, um die Auditingdaten anzeigen.

HINWEIS: Es kann bis zu zwei Minuten dauern, bis Änderungen an der Option **Überwachungsereignisse in das Ereignisprotokoll schreiben** wirksam wird. Wenn Sie darauf nicht warten wollen, starten Sie die Konsole neu.

So weisen Sie weiteren Benutzern die Rolle "Auditor" zu

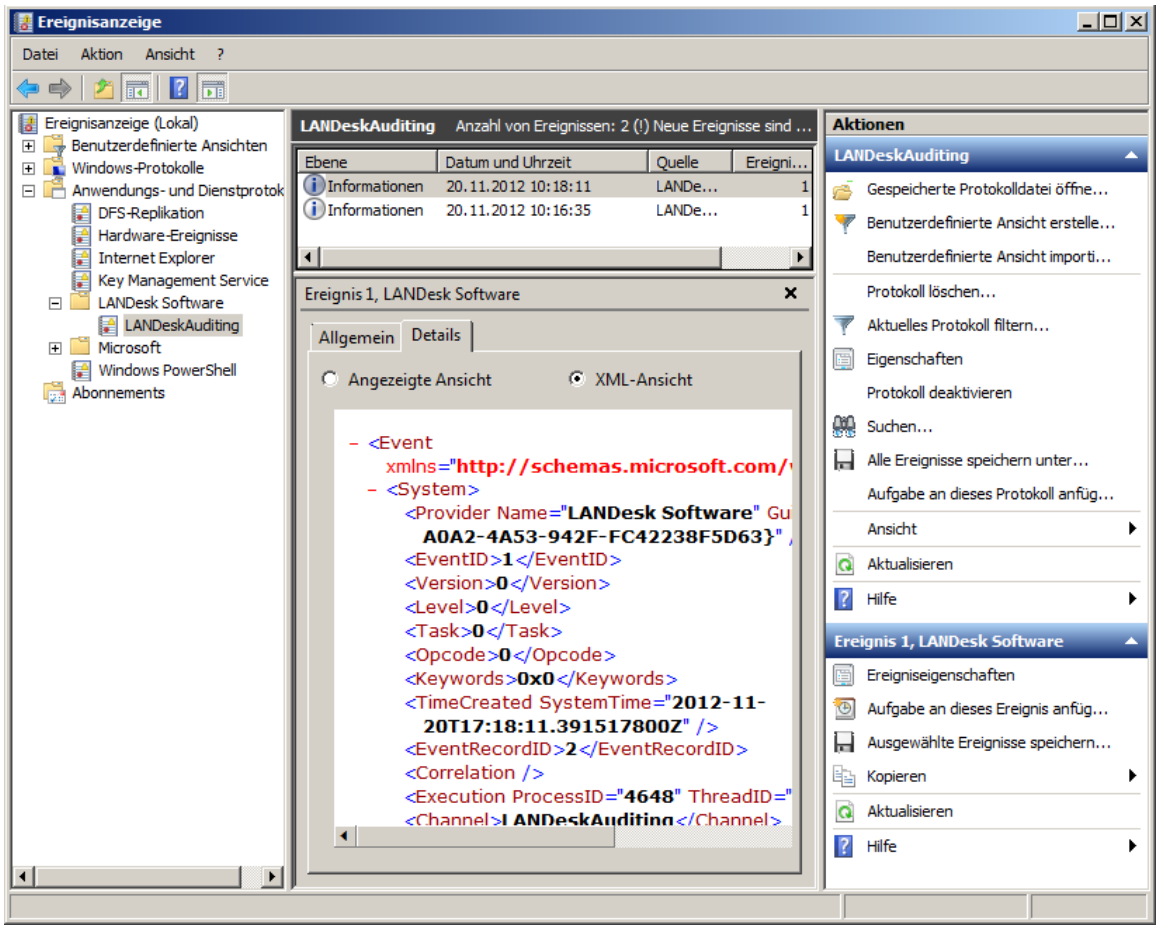
1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie im Baum **Rollen** doppelt auf **Auditor**.
3. Wählen Sie auf der Seite **Benutzer und Gruppen** die Benutzer aus, denen die Rolle "Auditor" zugewiesen werden soll.
4. Klicken Sie auf **OK**.
5. Veranlassen Sie die betreffenden Benutzer, ihre Konsole neu starten, damit sie das Extra "Auditing" sehen können.

Senden von Überwachungsereignissen an die Windows-Ereignisanzeige

LANDesk Management Suite speichert Überwachungsereignisse in der Coredatenbank. Sie können Überwachungsereignisse aber auch an die Anwendung "Windows-Ereignisanzeige" senden. Beachten Sie dabei, dass alle Benutzer mit Rechten zur Einsicht der Ereignisanzeige die Überwachungsprotokolleinträge sehen können. Sollte dies in Ihrer Umgebung ein Sicherheitsproblem darstellen, sollten Sie in Erwägung ziehen, die Überwachungsprotokolleinträge in der Ereignisanzeige zu schützen oder diese Option nicht zu aktivieren.

Management Suite protokolliert Überwachungsereignisse in folgendem Verzeichnis der Windows-Ereignisanzeige:

- Anwendungs- und Dienstprotokolle > LANDesk Software > LANDeskAuditing



So senden Sie Überwachungsereignisse an die Windows-Ereignisanzeige

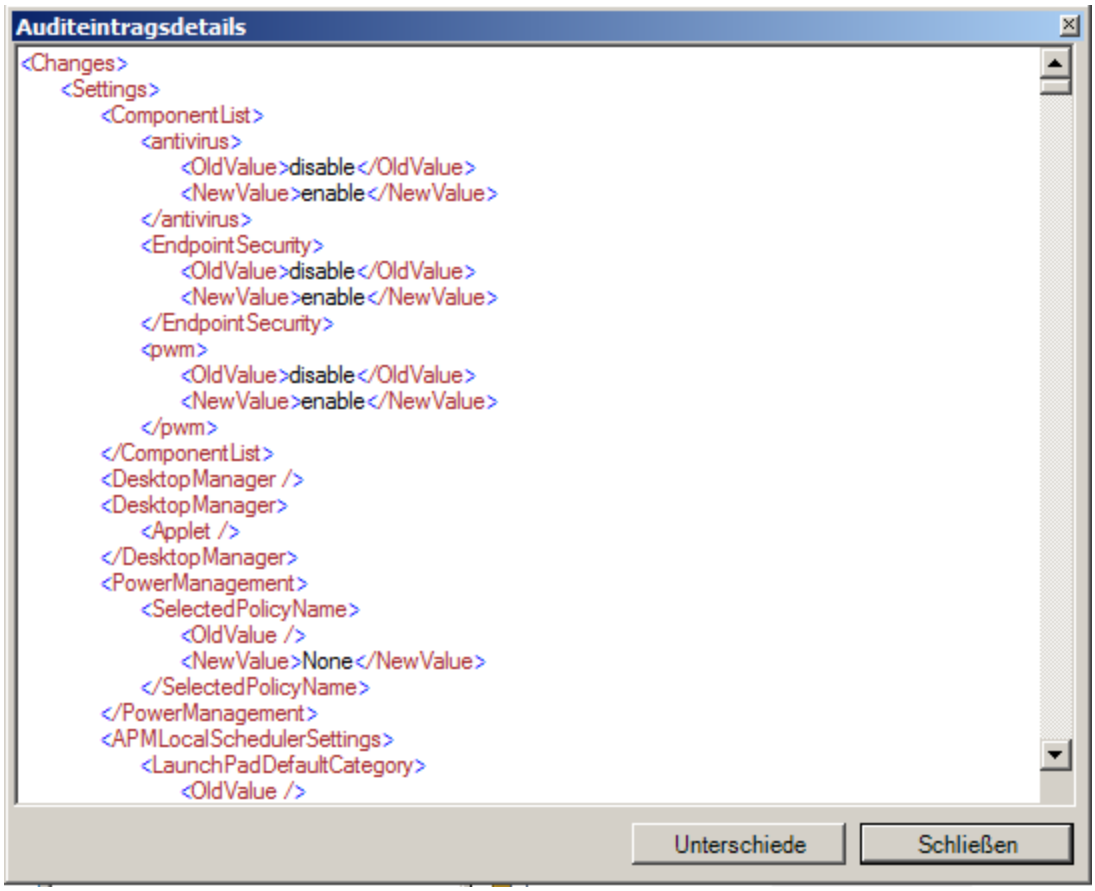
1. Klicken Sie auf **Extras > Dienste konfigurieren**.
2. Klicken Sie im Dialogfeld **LANDesk Softwaredienste konfigurieren** auf die Registerkarte **Überwachungskonfiguration** und wählen Sie **Überwachungsereignisse in das Ereignisprotokoll schreiben** aus. Falls diese Registerkarte nicht angezeigt wird, stellen Sie sicher, dass Ihnen die Rolle "Überwachungskonfiguration" zugewiesen wurde und Sie die Konsole im Anschluss an die Zuweisung dieser Rolle neu gestartet haben. Wenn Sie diese Option aktivieren, leuchtet kurz eine DOS-Box auf. Dies ist normal.
3. Klicken Sie auf **OK**.

Die Aktivierung der Protokollierung für die Ereignisanzeige wirkt sich nur auf Ereignisse aus, die nach der Aktivierung auftreten.

HINWEIS: Es kann bis zu zwei Minuten dauern, bis Änderungen an der Option **Überwachungsereignisse in das Ereignisprotokoll schreiben** wirksam wird. Wenn Sie darauf nicht warten wollen, starten Sie die Konsole neu.

Anzeigen von Überwachungsereignissen

Überwachungsereignisse werden im XML-Format in der Coredatenbank gespeichert. Wenn Sie auf ein Überwachungsereignis doppelklicken, um es zur Anzeige aufzurufen, werden die mit diesem Ereignis verknüpften, protokollierten XML-Elemente angezeigt. Welche Elemente protokolliert werden, hängt vom Überwachungsereignis ab.



Folgende Zeiträume werden von den Standardabfragen zu Überwachungsereignissen abgedeckt:

- die letzten 30 Tage
- die letzten 7 Tage
- der letzte Tag

So zeigen Sie Überwachungsereignisse mit Hilfe der Standardabfragen an

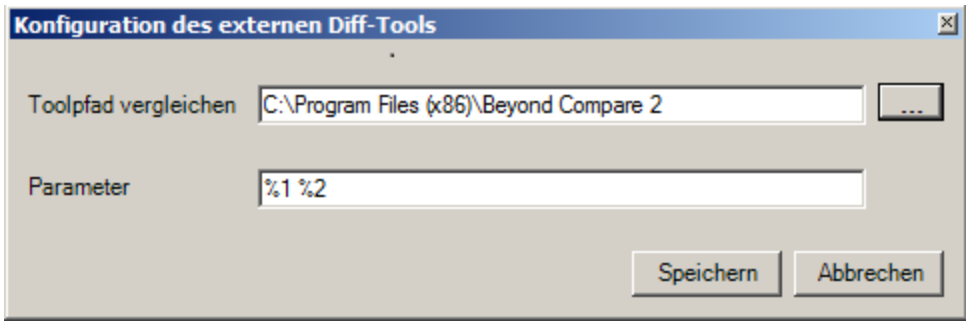
1. Klicken Sie auf **Extras > Administration > Auditing**.
2. Klicken Sie im Baum **Standardabfragen** auf die gewünschte Abfrage.

Sie können außerdem benutzerdefinierte Filter für die Auditabfragen erstellen. Weitere Informationen finden Sie unter "Erstellen von Filtern für Überwachungsereignisabfragen" auf Seite 207.

Identifizieren der Änderungen bei einem Überwachungsereignis

Manche Überwachungsereignisse können mit einer Vielzahl von Änderungen verbunden sein, so beispielsweise jene, die Änderungen der Agenteneinstellungen betreffen. In diesen Fällen kann es schwierig sein, aus dem XML-Code abzulesen, was sich bei dem überwachten Ereignis geändert hat.

Um diese Aufgabe zu vereinfachen bietet das Extra "Auditing" Unterstützung für ein Diff-Tool Ihrer Wahl, mit dem Sie eine XML-Datei zur einem Überwachungsereignis mit dem Status des Ereignisses vor seiner Änderung vergleichen können.



So konfigurieren Sie die Diff-Tool-Unterstützung für das Auditing

1. Klicken Sie auf **Extras > Administration > Auditing**.
2. Klicken Sie in der Auditing-Symbolleiste auf die Schaltfläche **Diff-Tool-Konfiguration eingeben**.
3. Geben Sie den **Pfad zum Vergeichstool** ein, der dem Speicherort der EXE-Datei Ihres Vergleichstools entspricht.
4. Passen Sie die Befehlszeile bei Bedarf für Ihr Diff-Tool an. "%1" steht für die ursprünglichen XML-Daten des ausgewählten Überwachungsereignisses und "%2" für die aktuellen XML-Daten des ausgewählten Überwachungsereignisses. Damit der Vergleich funktioniert, müssen beide Parameter "1%" und "%2" angegeben werden.
5. Klicken Sie auf die Schaltfläche **Speichern**.

So zeigen Sie die Unterschiede bei den XML-Daten des Überwachungsereignisses an

1. Doppelklicken Sie auf das Überwachungsereignis, das Sie auf Unterschiede prüfen wollen.
2. Klicken Sie im Dialogfeld **Auditeintragsdetails** auf die Schaltfläche **Unterschiede**.
3. Zeigen Sie die Unterschiede in dem von Ihnen konfigurierten Diff-Tool an.

Erstellen von Filtern für Überwachungsereignisabfragen

Der Ereignisverlauf für das Auditing wird innerhalb des Extras "Auditing" angezeigt (**Extras > Administration > Auditing**). Sie müssen entweder über die Rolle "Überwachungskonfiguration" oder die Rolle "Auditor" verfügen, damit dieses Extra für Sie in der Konsole angezeigt wird.

Sie können Filter für benutzerdefinierte Auditabfragen erstellen. Sie können unter folgenden Filtern für Überwachungsereignisse auswählen:

- **Benutzername:** Zeigt Überwachungsereignisse für den angegebenen Benutzernamen an.
- **Gerätename:** Zeigt Überwachungsereignisse für den angegebenen Gerätenamen an.

- **Änderungsdatum:** Zeigt Überwachungsereignisse innerhalb des angegebene Datumsbereichs oder innerhalb der angegebenen Anzahl von Tagen an.
- **Funktionen:** Zeigt Überwachungsereignisse für die ausgewählten Funktionen an. Sie müssen zunächst **Funktionen** auswählen, erst dann können Sie die Struktur für die **Ereignisse** erweitern.

Wenn Sie mehrere Filter auswählen, werden diese in der Abfrage als UND-Optionen behandelt. Wenn Sie beispielsweise einen Benutzernamen und eine Funktion auswählen, werden als Ergebnisse nur Geräte angezeigt, die sowohl mit diesem Benutzernamen als auch mit der ausgewählten Funktion übereinstimmen.

So erstellen Sie eine benutzerdefinierte Auditabfrage

1. Klicken Sie auf **Extras > Administration > Auditing**.
2. Klicken Sie auf das Strukturelement **Benutzerdefinierte Abfragen**.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Abfragedefinition**.
4. Ändern Sie die gewünschten Filter.
5. Wenn Sie fertig sind, klicken Sie auf **Erstellen**.

Berichte

Verwenden von Berichten

Mit dem Extra für die Berichterstellung können Sie detaillierte Berichten erstellen, die wichtige Informationen zu den Geräten in Ihrem Netzwerk liefern. Dieses Extra greift auf den Management Suite Inventarscanner zurück, mit dem Hardware- und Softwaredaten erfasst werden, um nützliche, aussagekräftige und aktuelle Berichte zu erstellen.

Es stehen mehrere Berichtstypen zur Verfügung:

- **(Vordefinierte) Standardberichte:** Im Lieferumfang von Management Suite enthaltene Standardberichte.
- **Benutzerdefinierte Berichte:** Benutzerdefinierte Berichte, die einen eindeutigen Satz von Informationen für die Generierung eines Berichts definieren. Mit dem integrierten Data Dynamics-Berichtsdesigner können Sie außerdem jeden Standardbericht Ihren spezifischen Anforderungen entsprechend anpassen.
- **Ad-hoc-Berichte:** Dies sind Berichte, die in verschiedenen Bereichen von Management Suite automatisch generiert werden können. So können Sie beispielsweise mit der rechten Maustaste auf eine Abfrage klicken und dann auf **Neuer Bericht**, um einen Bericht auf der Basis dieser Abfrage zu generieren.

Sie können Berichte so planen, dass sie in regelmäßigen Abständen ausgeführt werden. Geplante Berichte können veröffentlicht und auf einer geschützten Dateifreigabe auf dem Coreserver gespeichert werden. Dort können sie von jedem Benutzer, der über die entsprechenden Anmeldeinformationen verfügt, geöffnet und angezeigt werden. Sie können die veröffentlichten Berichte auch gemäß eines Zeitplans per E-Mail an ausgewählte Empfänger senden.

So starten Sie das Extra "Berichte"

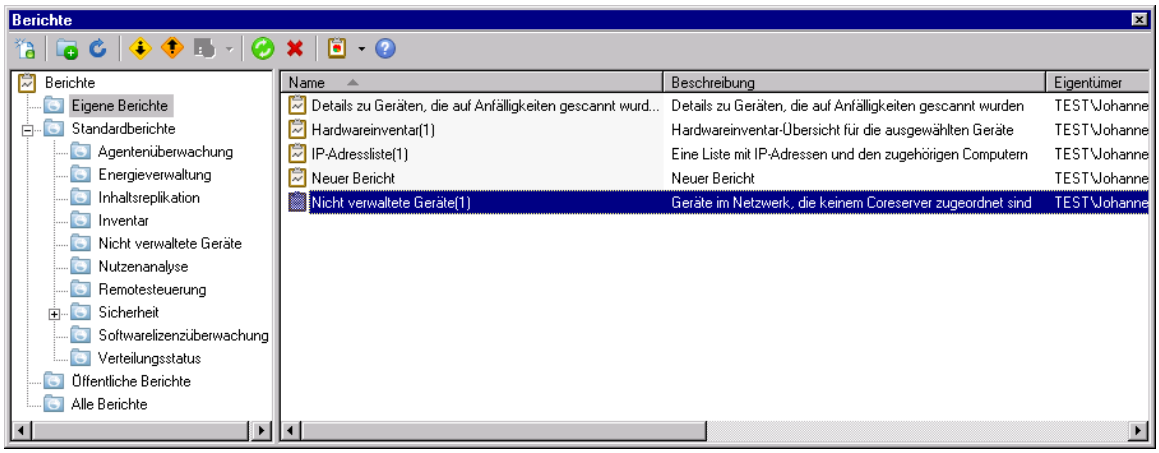
Klicken Sie auf **Extras > Berichte / Überwachung > Berichte**.

So verwenden Sie Berichte in der Webkonsole

Klicken Sie unterhalb der Gruppe **Berichte** auf **Berichte**.

Berichtsgruppen

Öffnen Sie das Extra "Berichte", um auf die vordefinierten Berichte zuzugreifen.



Berichte sind in einer Baumstruktur organisiert und in folgenden Ordnern zu Gruppen zusammengefasst:

- **Eigene Berichte:** Berichte, die der aktuelle Benutzer erstellt oder aus einem anderen Order kopiert hat. Dabei handelt es sich meistens um Berichte, die von Ihnen in regelmäßigen Abständen ausgeführt werden und die Sie Ihren Anforderungen entsprechend organisiert haben. Sie können die Berichte in Ordnern organisieren, die Sie erstellen. Ein Administrator hat Zugriff auf die Berichtgruppen eines Benutzers und kann Berichte hinzufügen und entfernen.
- **Standardberichte:** Vordefinierte Berichte, die zusammen mit der Management Suite installiert werden. Die Berichte sind formatiert, verfügen über ihnen zugeordnete Abfrageeigenschaften und Diagrammtypen und sind einsatzbereit.
- **Öffentliche Berichte:** Benutzerdefinierte Berichte, die für alle Benutzer auf dem Coreserver verfügbar gemacht werden.
- **Alle Berichte:** Alle Berichte, die vom aktuellen Benutzer verwendet werden können. Diese Ansicht weist auch ein Suchfeld auf, über das die Liste der Berichte gefiltert wird, wenn Sie einen Suchbegriff eingeben und eine Spalte auswählen. (Sie könnten beispielsweise "Lizenz" eingeben und die Spalte "Beschreibung" auswählen, um alle Berichte anzuzeigen, die im Zusammenhang mit Softwarelizenzen stehen.)

Administratoren können den Inhalt aller Berichtsgruppen einsehen. Benutzer mit Berichtsrecht können ebenfalls Berichte anzeigen, ausführen und veröffentlichen, jedoch nur auf den Geräten, die in ihrem Bereich enthalten sind. Benutzer mit dem Recht "Berichtsdesigner" können benutzerdefinierte Berichte erstellen.

Berichte werden gegen den Bereich und die Rechte des aktuell angemeldeten Benutzers abgeglichen. Wenn ein Benutzer nicht berechtigt ist, ein bestimmtes Extra zu verwenden, dann kann dieser Benutzer auch keine Berichte ausführen, die auf dieses Extra zurückgreifen. Analog hierzu werden in einen Bericht nur diejenigen Geräte einbezogen, die in den Bereich des Benutzers eingeschlossen sind.

Berichtsquellen

Vordefinierte Berichte erfassen Daten aus der Management Suite-Datenbank. Wenn Sie einen benutzerdefinierten Bericht erstellen, können Sie andere verfügbare Datenquellen angeben, die in den Bericht eingeschlossen werden sollen.

Berichtsformate

Wenn Sie einen Bericht ausführen, können Sie den Bericht in einem der folgenden Formate speichern:

- **HTML:** Standard-HTML. Sie können Diagramme in HTML-Berichten anklicken, wenn Sie detaillierte Informationen zu einem Element anzeigen möchten.
- **Bild:** Bitmap-Bilddatei
- **PDF:** Adobe PDF-Datei
- **XML:** Textdatei im XML-Format
- **DOC:** Microsoft Word
- **XLS:** Microsoft Excel

Wenn Sie einen Bericht im Extra "Berichte" planen, können Sie die folgenden Formate verwenden:

- **PDF:** Adobe PDF-Datei
- **XLS:** Microsoft Excel
- **DOC:** Microsoft Word
- **CSV:** Textdatei mit durch Kommas getrennten Werten.

Zusätzliche Ressourcen für Berichte

Nähere Informationen zum Einsatz von Management Suite Berichten finden Sie im Berichtsportal der LANDesk User Community unter community.landesk.com/ldmsreports. Das Berichtsportal bietet zusätzliche Dokumentation, Kundenfragen und Berichte zum Download. Alle LANDesk Benutzer können benutzerdefinierte Berichte einreichen und der gesamten Community zur Nutzung zur Verfügung stellen.

Schnellen Zugriff auf das Berichtsportal der LANDesk User Community erhalten Sie, wenn Sie auf **Extras > Berichte / Überwachung > Community-Berichte** klicken.

Erforderliche Rechte für die Verwendung von Berichten

Nicht alle Benutzer können Berichte anzeigen, bearbeiten und bereitstellen. Benutzern müssen in der rollenbasierten Administration die richtigen Rechte zugewiesen sein. Da die Bearbeitung von Berichten ein Zugreifen des Benutzers auf die Datenbank bedeutet, muss jeder Benutzer mit dem Recht "Bearbeiten" qualifiziert sein, die Datenbank zu bearbeiten. Sie können ferner Anmeldeinformationen einrichten, die Benutzern lediglich ein Leserecht für die Daten in der Datenbank einräumen, wenn es Benutzer gibt, die Berichte ausführen aber nicht bearbeiten sollen.

Rollenbasierte Administration and Berichte

Die rollenbasierte Administration schließt Rechte zur Berichterstellung ein, die festlegen, welcher Benutzer Berichte anzeigen, ausführen, ändern, planen und erstellen kann. Wenn Sie im Extra "Benutzerverwaltung" eine Rolle erstellen oder bearbeiten, können Sie die folgenden Berechtigungen für Berichte aktivieren oder deaktivieren

Berechtigungen		Ansicht	Bearbe	Bereitste	Öffentlich bearbeiten
Berichte	✗				
Berichte		✗	✗	✗	✗
Berichtsdesigner		⊘	✗	⊘	⊘

Berichtsdesigner

- Keine Rechte: Kann den Designer nicht öffnen.
- Bearbeiten: Kann den Designer öffnen und Berichte erstellen oder bearbeiten.

Berichte

- Keine Rechte: Kann das Extra nicht sehen.
- Ansicht: Kann dieses Extra sehen und Berichte anzeigen. Kann Berichte ausführen. Kann keinerlei Änderungen vornehmen.
- Bearbeiten: Kann Berichte anzeigen und Berichtseigenschaften ändern. Dieses Recht alleine gewährt keinen Zugriff auf den Designer. Für den Zugriff auf den Berichtsdesigner ist das Recht "Bearbeiten" erforderlich.
- Bereitstellen: Kann Bericht planen und veröffentlichen.
- Öffentlich bearbeiten: Kann Berichte in die Gruppe "Öffentlich" verschieben.

Benutzerdatenbankrechte für Berichte

Der Berichtsdesigner ist ein leistungsstarkes Tool, das mit Umsicht verwendet werden sollte. Benutzer, die das Recht " Bearbeiten" für den Berichtsdesigner besitzen, können auf alle Teile der Datenbank zugreifen und jeden beliebigen SQL-Befehl für diese Daten ausführen. Sie sollten also sicherstellen, dass Benutzer, die mit diesem Recht ausgestattet sind, auch wirklich qualifiziert sind, die Datenbank zu verwalten. Wenn ein Benutzer SQL-Befehle ausführt, die zu Datenänderungen führen, könnten Daten verloren gehen oder beschädigt werden.

Das Extra "Berichte" greift mit den Benutzeranmeldeinformationen auf die Datenbank zu, die beim Produktsetup festgelegt wurden. Diese Anmeldeinformationen können über das Dialogfeld **LANDesk Softwaredienste konfigurieren** verwaltet werden. Wenn Sie es vorziehen, andere Anmeldeinformationen für Benutzer einzurichten, die Berichterstellungsrechte haben, können Sie einen zweiten Satz Anmeldeinformationen für den Zugriff auf die Berichtsdatenbank erstellen.

Angenommen, Sie möchten Berichtsbenutzern lediglich Leserechte für die Datenbank geben, dann können Sie ein Datenbankbenutzerkonto einrichten, dass nur den Lesezugriff gestattet. Sie würden dann das betreffende Benutzerkonto im Dialogfeld **LANDesk Softwaredienste konfigurieren** als Berichtsdatenbankbenutzer eingeben.

HINWEIS: Wenn Sie eine Oracle-Datenbank verwenden und einen Berichtsbenutzer erstellen, der nur Leserechte hat, müssen Sie ein öffentliches Synonym für jede Tabelle erstellen, die von den Berichten dieses Benutzers referenziert wird.

Verwandte Themen

"Erstellen eines Benutzers mit Berichterstellungsrechten" auf Seite 212

Erstellen eines Benutzers mit Berichterstellungsrechten

Das Extra "Berichte" greift mit den Benutzeranmeldeinformationen auf die Datenbank zu, die beim Produktsetup festgelegt wurden. Wenn Sie es vorziehen, andere Anmeldeinformationen für Benutzer einzurichten, die Berichterstellungsrechte haben, können Sie einen zweiten Satz Anmeldeinformationen für den Zugriff auf die Berichtsdatenbank erstellen.

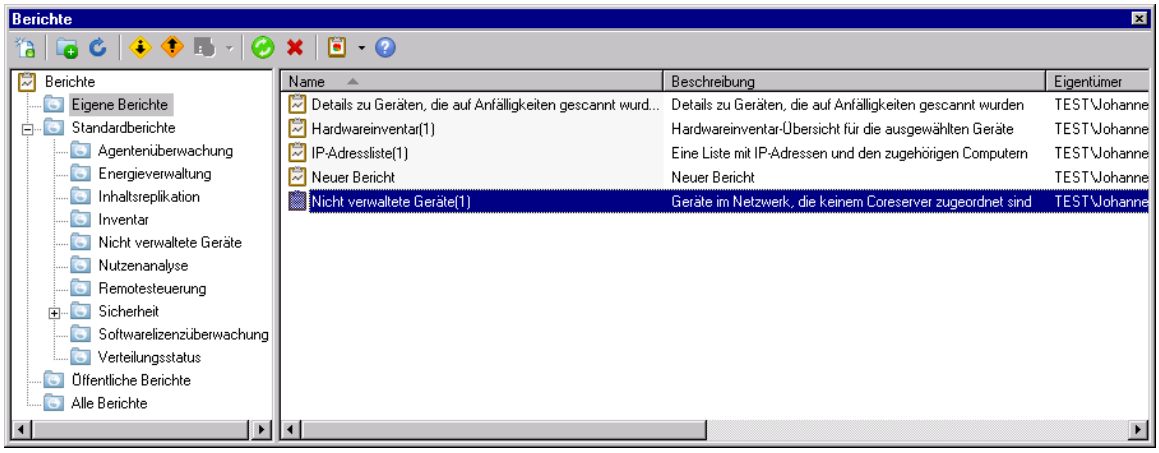
So definieren Sie die Anmeldeinformationen für Berichtsdatenbankbenutzer

1. Erstellen Sie ein Benutzerkonto für Ihre Datenbank und weisen Sie diesem die gewünschten Rechte zu.
2. Klicken Sie in der Management Suite Konsole auf **Konfigurieren > Dienste**.

3. Geben Sie unter **Berichtsdatenbankbenutzer** den Benutzernamen und das Kennwort für dieses Konto ein.
4. Klicken Sie auf **OK**.

Ausführen von Berichten

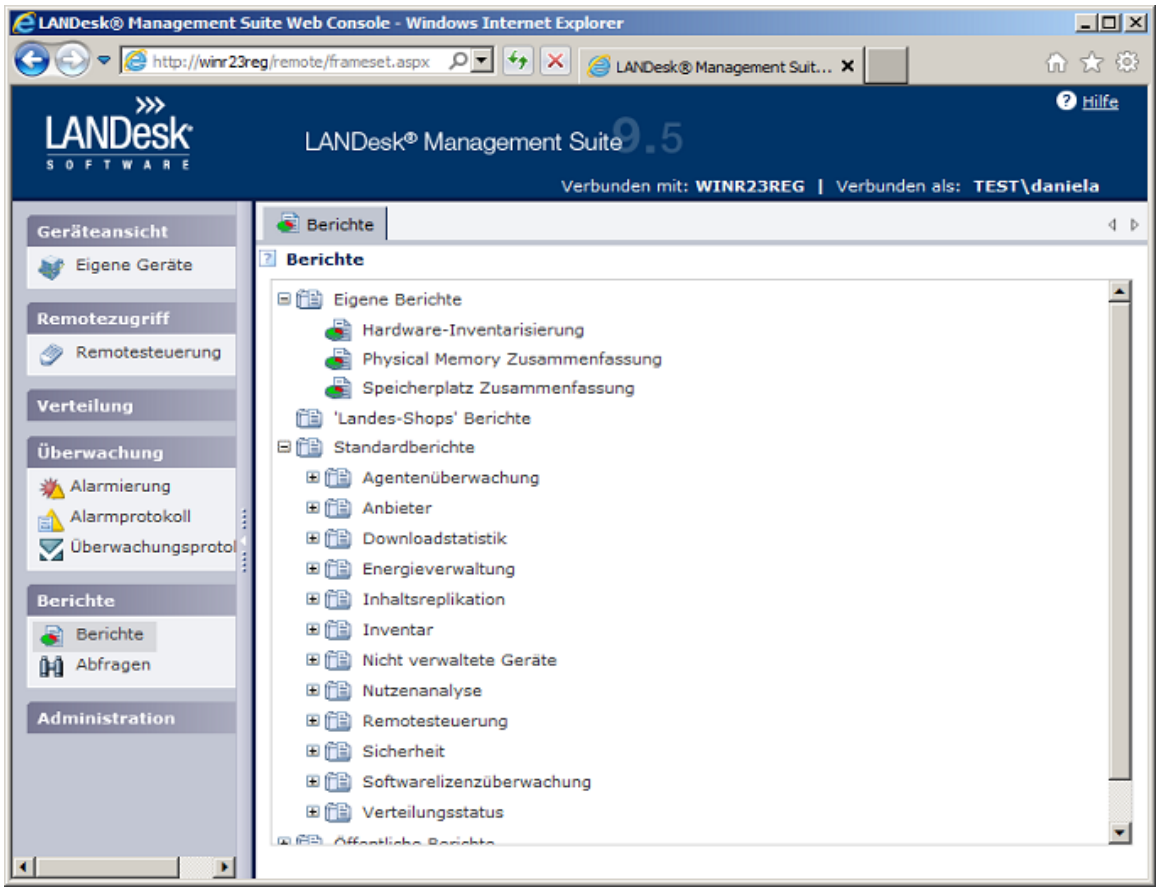
Das Extra "Berichte" verwenden Sie zum Ausführen und Organisieren von Berichten und zur Erstellung neuer Berichte. Sie können Berichte zeitlich so planen, dass sie nur einmal oder aber in regelmäßigen Abständen ausgeführt werden. Sie können Berichte auch zur Verwendung auf anderen Management Suite-Konsolen importieren und exportieren.



Am schnellsten können Sie Berichtsdaten anzeigen, wenn Sie den Bericht von einer Konsole ausführen. Der Bericht-Viewer (die Berichtsansicht) zeigt die Daten entweder in Form einer Vorschau der gedruckten Seite oder als kontinuierliche Daten an. Sie können die Ansichten und Formate im Bericht-Viewer ändern. Sie können auch die Berichtsparameter dahingehend ändern, dass Sie eine Untermenge an Daten auswählen.

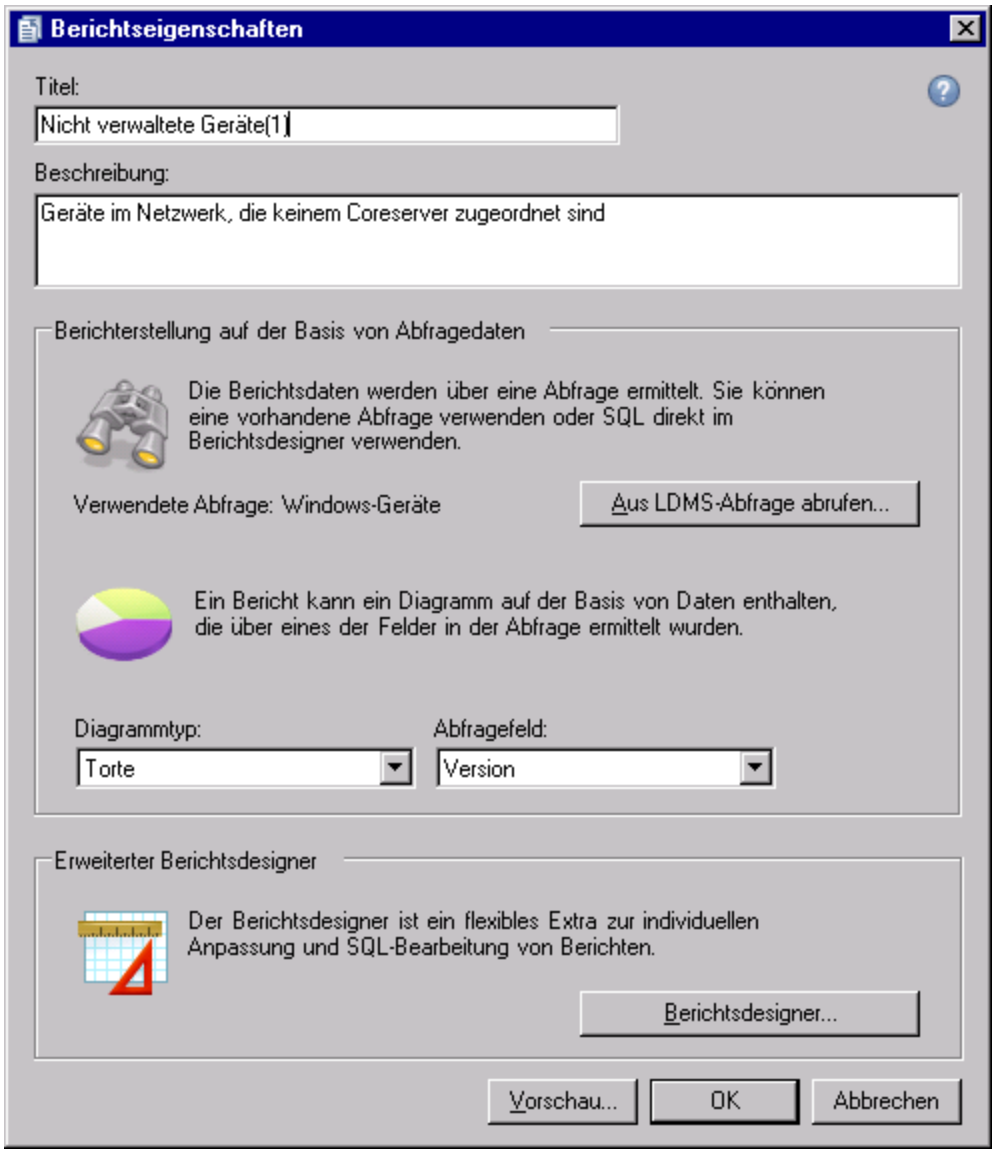
Berichte in der Webkonsole

Wenn Sie die Webkonsole verwenden, stehen Ihnen die Berichte der Windows-Konsole zur Verfügung, wobei jedoch geringfügige Unterschiede in der Art und Weise bestehen, in der Parameter angezeigt und ausgewählt werden. Sie können in der Webkonsole keine benutzerdefinierten Berichte bearbeiten oder erstellen oder Berichte zwischen Ordnern verschieben, wohl aber Berichte ausführen, anzeigen und exportieren.



Ändern von Berichtseigenschaften

Sie können eine Kopie eines vordefinierten Berichts erstellen und Elemente im Dialogfeld **Berichtseigenschaften** ändern. Sie können die Art des im Bericht angezeigten Diagramms ändern und ein anderes Abfragefeld als das Schlüsselelement in der Abfrage definieren. Sie können auch eine LDMS Abfrage als Grundlage für den Bericht auswählen. Außerdem können Sie den Namen und die Beschreibung ändern.


Berichtseigenschaften
Titel:
Nicht verwaltete Geräte(1)
Beschreibung:
Geräte im Netzwerk, die keinem Coreserver zugeordnet sind
Berichterstellung auf der Basis von Abfragedaten
Die Berichtsdaten werden über eine Abfrage ermittelt. Sie können eine vorhandene Abfrage verwenden oder SQL direkt im Berichtsdesigner verwenden.
Verwendete Abfrage: Windows-Geräte
Aus LDMS-Abfrage abrufen...
Ein Bericht kann ein Diagramm auf der Basis von Daten enthalten, die über eines der Felder in der Abfrage ermittelt wurden.
Diagrammtyp:
Torte
Abfragefeld:
Version
Erweiterter Berichtsdesigner
Der Berichtsdesigner ist ein flexibles Extra zur individuellen Anpassung und SQL-Bearbeitung von Berichten.
Berichtsdesigner...
Vorschau...
OK
Abbrechen

Wenn Sie umfangreichere Änderungen an dem Bericht vornehmen wollen, müssen Sie hierzu den Berichtsdesigner aufrufen.

Einzelheiten zur Verwendung des Berichtsdesigners See "Erstellen von benutzerdefinierten Berichten" on page 227.

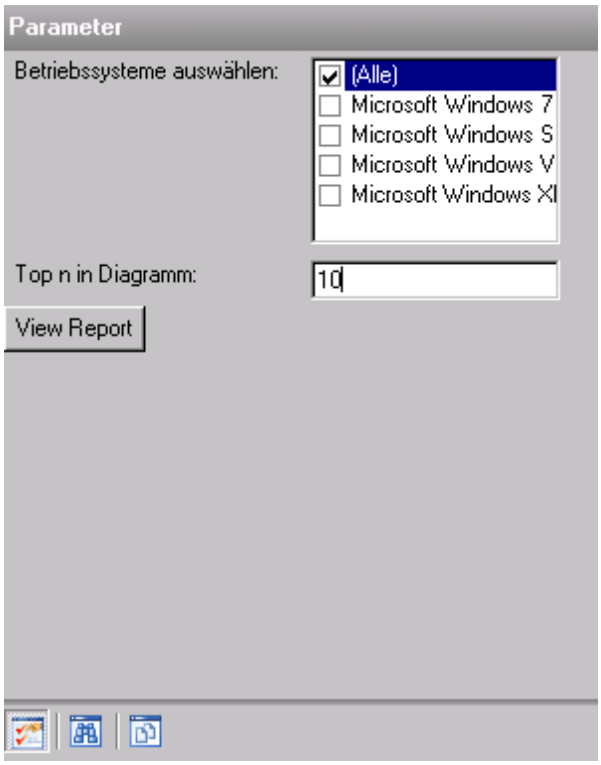
Bericht-Viewer

Wenn Sie einen Bericht ausführen, wird der Bericht-Viewer gestartet und der generierte Bericht wird angezeigt. Mit den Steuerschaltflächen des Bericht-Viewers können Sie den Bericht Ihren Anforderungen entsprechend darstellen. Sie können einen Bericht vom Bericht-Viewer aus auch exportieren oder zur Verteilung in einem anderen Format speichern.

Der Bericht-Viewer besitzt eine Symbolleiste und eine Randleiste. Die Symbolleiste umfasst die folgenden Schaltflächen:

- **Öffnen:** Hiermit wird ein gespeicherter Bericht im Viewer geöffnet.
- **Exportieren:** Speichert den Bericht als Bild (im Format BMP, EMF, GIF, JPEG, TIFF oder PNG) oder im HTML-, PDF-, XML-, XLS- oder DOC-Format.
- **Kopieren:** Kopiert den Inhalt des Berichts für die ausgewählte Seite.
- **Druckvorschau:** Dient zum Umschalten der Druckvorschau (Seitenansicht). Ist diese Schaltfläche nicht aktiviert, wird der Bericht als einzelne HTML-Seite angezeigt.
- **Seiteneinrichtung:** Dient zur Änderung der Einstellungen für Seite, Layout und Wasserzeichen.
- **Drucken:** Öffnet das Standarddialogfeld der Druckfunktion.
- **Randleistenbereich:** Dient zur Umschaltung des Randleistenbereichs, in dem Such- und Parameteroptionen und Miniaturansichten angezeigt werden.
- **Zurück zum übergeordneten Bericht:** Wenn Sie gerade einen untergeordneten Bericht anzeigen, kehren Sie hiermit zum übergeordneten Bericht zurück, von dem aus der Unterbericht abgerufen wurde.
- **Keine:** Standardmausbewegungen für die Ansicht verwenden.
- **Schwenkmodus:** Ziehen Sie am Handzeiger, um die Seite in eine beliebige Richtung zu schwenken bzw. zu verschieben.
- **Auswahlmodus:** Ziehen Sie den Zeiger, um einen Teil der Seite auszuwählen. Sie können die Auswahl in eine andere Anwendung einfügen, die das Einfügen von Text unterstützt.
- **Snapshot-Modus:** Ziehen Sie den Zeiger, um ein Rechteck auszuwählen. Sie können das Rechteck in eine andere Anwendung einfügen, die das Einfügen von Bildern unterstützt.
- **Vergrößern:** Vergrößert den Bericht.
- **Verkleinern:** Verkleinert den Bericht.
- **Zoom-Prozentsatz:** Hiermit können Sie die Darstellungsgröße des Berichts bestimmen.
- **Erste Seite:** Hiermit zeigen Sie die erste Seite des Berichts an.
- **Vorherige Seite:** Hiermit zeigen Sie die vorherige Seite des Berichts an.
- **Seitenfeld:** Hiermit fügen Sie eine bestimmte Seitenzahl ein, mit der Sie direkt zu der betreffenden Seite gelangen.
- **Nächste Seite:** Hiermit zeigen Sie die nächste Seite in der Seitenabfolge an.
- **Letzte Seite:** Hiermit zeigen Sie die letzte Seite des Berichts an.
- **Abbrechen:** Beendet die Ausführung des Berichts. Wenn die Ausführung des Berichts bereits abgeschlossen ist, wird diese Schaltfläche abgeblendet angezeigt.
- **Aktualisieren:** Kehrt zur ursprünglichen Ansicht zurück.
- **Suchen:** Öffnet den Suchbereich, der dazu dient, eine bestimmte Textzeichenfolge innerhalb der Berichtsdaten zu finden.

Die Randleiste bietet drei Optionen, auf die mittels der Symbole am unteren Rand der Leiste zugegriffen werden kann.



- **Parameter:** Dient zur Änderung von Parametern des Berichts zwecks Auswahl eines Teilsatzes der Daten und Abwandlung der Ergebnisse je nach Definition des Berichts. Sobald Sie andere Parameter ausgewählt haben, klicken Sie auf **Bericht anzeigen**, um den Bericht mit den neuen Parametern zu aktualisieren.
- **Suchergebnisse:** Sucht nach einer Zeichenfolge in den Berichtsergebnissen. Geben Sie die Zeichenfolge ein und wählen Sie ein beliebiges Kriterium aus (wie z. B. Groß-/Kleinschreibung beachten) und klicken Sie auf **Suchen**. Daraufhin wird eine Liste mit den Vorkommen der Zeichenfolge angezeigt. Klicken Sie auf ein Vorkommen, um zum entsprechenden Abschnitt des Berichts zu gelangen. Das Auftreten der entsprechende Zeichenfolge wird hervorgehoben dargestellt. Sie können auch auf einen grünen Balken entlang des rechten Rands des Berichts klicken, um von einem Vorkommen zum nächsten zu gelangen.
- **Seitenminiaturansichten:** Zeigt Miniaturansichten der Berichtsseiten an. Klicken Sie auf eine Miniaturansicht, um zur betreffenden Seite zu wechseln.

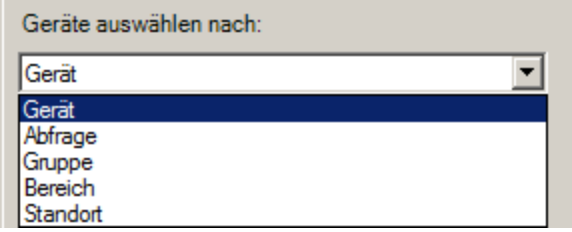
Auswählen von Parametern aus einer Liste

Wenn die Randleiste eine Liste mit Parametern enthält, können Sie alle Listenelemente in den Bericht einbeziehen, indem Sie das Kontrollkästchen **Alle** markieren. Wenn Sie dies tun, werden die Kontrollkästchen für die einzelnen Elemente zwar nicht markiert, aber dennoch werden alle Elemente in den Bericht eingeschlossen.

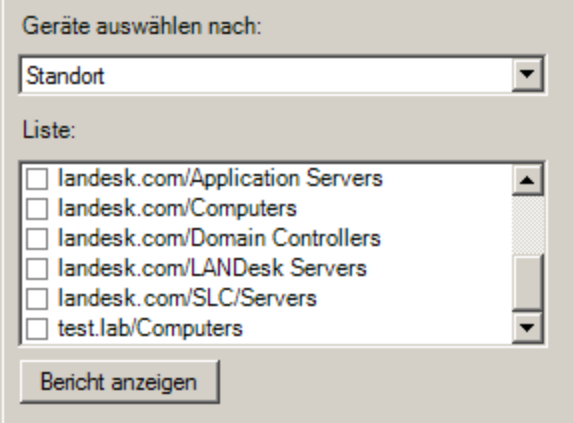
Um eine Teilmenge der Elemente auszuwählen, löschen Sie das Kontrollkästchen **Alle** und aktivieren dann die Kontrollkästchen neben den einzelnen Elementen, die in den Bericht einbezogen werden sollen.

Auswählen von Geräten, Gruppen oder Standorten

Die Parameter variieren je nach Bericht. Alle Berichte enthalten aber eine Option zur Geräteauswahl, mit der einzelne Geräte, Abfragen, Gruppen, der Bereich oder Standort festgelegt wird. Auf diese Weise können Sie einen Bericht für eine Abfrage, eine Gruppe oder einen Bereich generieren, die bzw. den Sie in der Netzwerkansicht definiert haben, oder aber für einen Standort innerhalb Ihres Netzwerks.



So können Sie beispielsweise Geräte an einem Standort anhand des Gerätenetzwerkstandorts auswählen. Wenn Sie "Standort" auswählen, werden in der Liste Standorte in Ihrem Netzwerk nach Domänenname geordnet angezeigt.



Unterberichte

Manche Berichte können sekundäre Berichte oder Unterberichte aufrufen. Unter dem Order "Sicherheit" gibt es Berichte im Dashboardstil für Antivirus und Anfälligkeiten. Wenn Sie den Dashboardbericht (oder übergeordneten Bericht) öffnen, können Sie auf eines der Diagramme klicken, um den zugehörigen Unterbericht (oder untergeordneten Bericht) aufzurufen.

Angenommen, Sie führen den Dashboardbericht zu Antivirus aus, dann klicken Sie auf das Diagramm "Echtzeit-Scannerstatus", um einen separaten Bericht zum Gerätescanstatus aufzurufen. Sie können dann auf die Schaltfläche **Zurück zum übergeordneten Bericht** klicken, um zum Dashboardbericht zurückzukehren.

Ausführen eines Berichts

Wenn Sie einen Bericht ausführen, zeigt der Bericht-Viewer (die Berichtsansicht) die Daten entweder in Form einer Vorschau der gedruckten Seite oder als kontinuierliche Daten an. Sie können die Ansichten und Formate im Bericht-Viewer ändern. Sie können auch die Berichtsparameter dahingehend ändern, dass Sie eine Untermenge an Daten auswählen.

1. Wählen Sie im Extra **Berichte** einen Ordner in der Baumstruktur "Berichte" aus und suchen Sie den gewünschten Bericht.
2. Doppelklicken Sie auf den Bericht.

   Das Dialogfeld "Berichtsvorschau" wird aufgerufen. Manche Berichte besitzen konfigurierbare Parameter, mit denen Sie eine Untermenge an Daten für den Bericht auswählen können. Liegen keine Standardparameter vor, müssen Sie mindestens einen Parameter definieren (z. B. den Gerätenamen angeben), sonst enthält der Bericht keine Daten.

3. Stehen Parameter zur Auswahl, geben Sie die gewünschten Parameter an.
4. Klicken Sie auf **Bericht anzeigen**.
5. Wenn Sie Details zu einem bestimmten Bereich eines Diagramms anzeigen möchten, klicken Sie auf den betreffenden Bereich im Diagramm. In der Ansicht wird daraufhin der Abschnitt des Berichts angezeigt, der den Daten in diesem Bereich des Diagramms entspricht.
6. Klicken Sie in Berichtsseiten auf die Spaltenpfeile , um die Daten nach der betreffenden Spalte zu sortieren.
7. Die Schaltflächen in der Symbolleiste verwenden Sie für die Suche nach Daten, den Export von Daten in ein anderes Format, das Drucken des Berichts usw.
8. Wenn Sie fertig sind, schließen Sie das Vorschau-Browserfenster.

HINWEIS: Wenn Sie Geräte mithilfe des Parameters "Gerät" auswählen, wird kein Platzhalter verwendet. Geben Sie eine beliebige Anzahl von Zeichen an, die in allen Gerätenamen enthalten sind, die in Ihrer Auswahl enthalten sein sollen und klicken Sie auf **Bericht anzeigen**. Alle Gerätenamen, die die von Ihnen angegebene Zeichenfolge enthalten, werden in den Bericht einbezogen.

Auswählen von Parametern aus einer Liste

Wenn die Randleiste eine Liste mit Parametern enthält, können Sie alle Listenelemente in den Bericht einbeziehen, indem Sie das Kontrollkästchen **Alle** markieren. Wenn Sie dies tun, werden die Kontrollkästchen für die einzelnen Elemente zwar nicht markiert, aber dennoch werden alle Elemente in den Bericht eingeschlossen.

Um eine Teilmenge der Elemente auszuwählen, löschen Sie das Kontrollkästchen **Alle** und aktivieren dann die Kontrollkästchen neben den einzelnen Elementen, die in den Bericht einbezogen werden sollen.

Speichern eines Berichts in einer Datei

Nachdem Sie einen Bericht ausgeführt haben, können Sie die Ergebnisse in einer Datei speichern. Der Bericht kann als Bild (im Format BMP, EMF, GIF, JPEG, TIFF oder PNG) oder im HTML-, PDF-, XML-, XLS- oder DOC-Format gespeichert werden.

1. Führen Sie einen Bericht aus.
2. Klicken Sie in der Symbolleiste des Viewers auf die Schaltfläche **Exportieren**.
3. Klicken Sie auf das Berichtsformat, das Sie verwenden möchten.
4. Ändern Sie im Dialogfeld **Exportieren** ggf. die Parameter für den Bericht. (Die Parameter variieren je nachdem, welches Format ausgewählt wurde.)

5. Wechseln Sie in das Verzeichnis, indem Sie den Bericht speichern möchten, geben Sie einen Namen für den Bericht ein und klicken Sie auf **Speichern**.
6. Klicken Sie auf **Exportieren**.

HINWEIS: Wenn Sie einen Bericht speichern und planen, diesen per E-Mail zu versenden, sollten Sie anstelle der HTML-Ausgabe vorzugsweise das PDF-Format verwenden.

Planen von Berichten

Wenn Sie einen bestimmten Bericht regelmäßig benötigen, können Sie ihn so planen, dass er vorzeitig oder außerhalb der üblichen Arbeitszeiten ausgeführt wird, wenn die Coredatenbank möglicherweise nicht so stark belastet ist. Wenn Sie einen Bericht planen, wird dieser in der LANDesk Berichte-Freigabe (ldmain\reports) gespeichert und auch an alle Benutzer des Coreservers gesendet, die über Berichtsrechte verfügen und für die (im Extra "Benutzerverwaltung") eine E-Mail-Adresse mit dem Benutzernamen verknüpft ist. Damit Sie Berichte per E-Mail versenden können, benötigen Sie einen SMTP-Server.

Ein Bericht, der in der Berichte-Freigabe gespeichert wird, basiert auf dem Bereich der Person, die ihn zeitlich geplant hat. Bei Berichten, die an andere Empfänger gesendet werden, verwendet der Bericht den Bereich des jeweiligen Empfängers zur Filterung der Daten.

Um einen Bericht planen zu können, muss ein Benutzer das Recht "Berichte - Bereitstellen" besitzen.

Wenn Sie einen Bericht verteilen möchten, den Sie ausgeführt haben, speichern Sie den Bericht in dem gewünschten Format und fügen diese Datei dann an als Anhang zu einer E-Mail-Nachricht hinzu. Bei dem Bericht wird dann Ihr Bereich verwendet. Benutzer mit Zugriffsrechten auf die Berichte-Freigabe können den Bericht auch von diesem Speicherort aus anzeigen.

HINWEIS: Wenn Sie einen Bericht speichern und planen, diesen per E-Mail zu versenden, sollten Sie anstelle der HTML-Ausgabe vorzugsweise das PDF-Format verwenden.

HINWEIS: Die Ausführung umfangreicher Berichte mit vielen Daten kann große Mengen an Systemressourcen auf dem Coreserver beanspruchen. Deshalb kann immer nur ein Bericht geplant werden. Wenn bereits ein Bericht ausgeführt wird und Sie planen zur gleichen Zeit andere Berichte, werden der zweiten Bericht und nachfolgende Berichte so lange verzögert, bis der erste Bericht abgeschlossen ist.

Planen eines Berichts

1. Blenden Sie im Extra **Berichte** die Baumstruktur ein und wählen Sie einen Bericht zur Planung aus.
2. Klicken Sie in der Symbolleiste auf **Planen** und wählen Sie das Format aus, das Sie verwenden möchten.

   Das Extra **Geplante Tasks** wird geöffnet und der Bericht ist ausgewählt.

3. Klicken Sie auf die Schaltfläche **Eigenschaften** in der Symbolleiste.
4. Geben Sie im Dialogfeld **Task planen** die Informationen auf allen Seiten ein oder bearbeiten Sie diese.
5. Klicken Sie auf **Speichern**.

Sie können den Fortschritt des Berichts im Extra **Geplante Tasks** einsehen. (Klicken Sie hierzu auf den Ordner **Eigene Tasks**.)

Eine Beschreibung der Optionen im Dialogfeld "Task planen" finden Sie unter "Informationen zum Dialogfeld "Task planen"" auf Seite 240.

Ändern der Eigenschaften eines Berichts

1. Kopieren Sie im Extra **Berichte** einen Bericht und fügen Sie die Kopie in einen Ordner ein.
2. Klicken Sie mit der rechten Maustaste auf den Bericht und wählen Sie **Eigenschaften** aus.
3. Ändern Sie im Dialogfeld **Berichtseigenschaften** die gewünschten Eigenschaften.
4. Klicken Sie auf **Vorschau**, um den angepassten Bericht im Bericht-Viewer anzuzeigen.
5. Klicken Sie auf **OK**, um den geänderten Bericht zu speichern.

Anpassen einer Berichtsvorlage

Sämtliche Berichte bauen auf Vorlagen auf, die im Lieferumfang der LANDesk Management Suite enthalten sind. Wenn Sie eine Berichtsvorlage anpassen möchten, müssen Sie die Mastervorlagendatei im Berichtsdesigner öffnen. Beispielsweise könnte es sein, dass Sie den Namen und das Logo Ihres Unternehmens zur Vorlage hinzufügen oder das zugrunde liegende Seitenlayout, die Schriftart oder andere Elemente ändern wollen

Drei Vorlagendateien stehen zur Verfügung: eine im Hochformat, eine im Querformat und eine Dashboard-Vorlage.

HINWEIS: Berichtsvorlagen werden auf jedem Gerät installiert, auf dem Sie die Konsole installieren. Wenn Sie ein Vorlage auf dem Coreserver ändern, wird diese Vorlage beim Ausführen von Berichten auf dem Core und von der Webkonsole verwendet. Andere Konsolen verwenden hingegen die Vorlage, die auf ihnen installiert wurde. Wenn Sie eine überarbeitete Vorlage auf anderen Konsolen verwenden möchten, müssen Sie die Vorlagendatei auf jede weitere Konsole kopieren oder einen Verteilungstask erstellen, mit dem die Vorlagendateien verteilt werden.

So passen Sie eine Berichtsvorlage an

1. Klicken Sie im Extra **Berichte** in der Symbolleiste auf die Schaltfläche **Vorlage bearbeiten**.
2. Wählen Sie eine der Optionen Hochformat, Querformat oder Dashboard aus.

   Die Vorlage wird im Berichtsdesigner geöffnet.

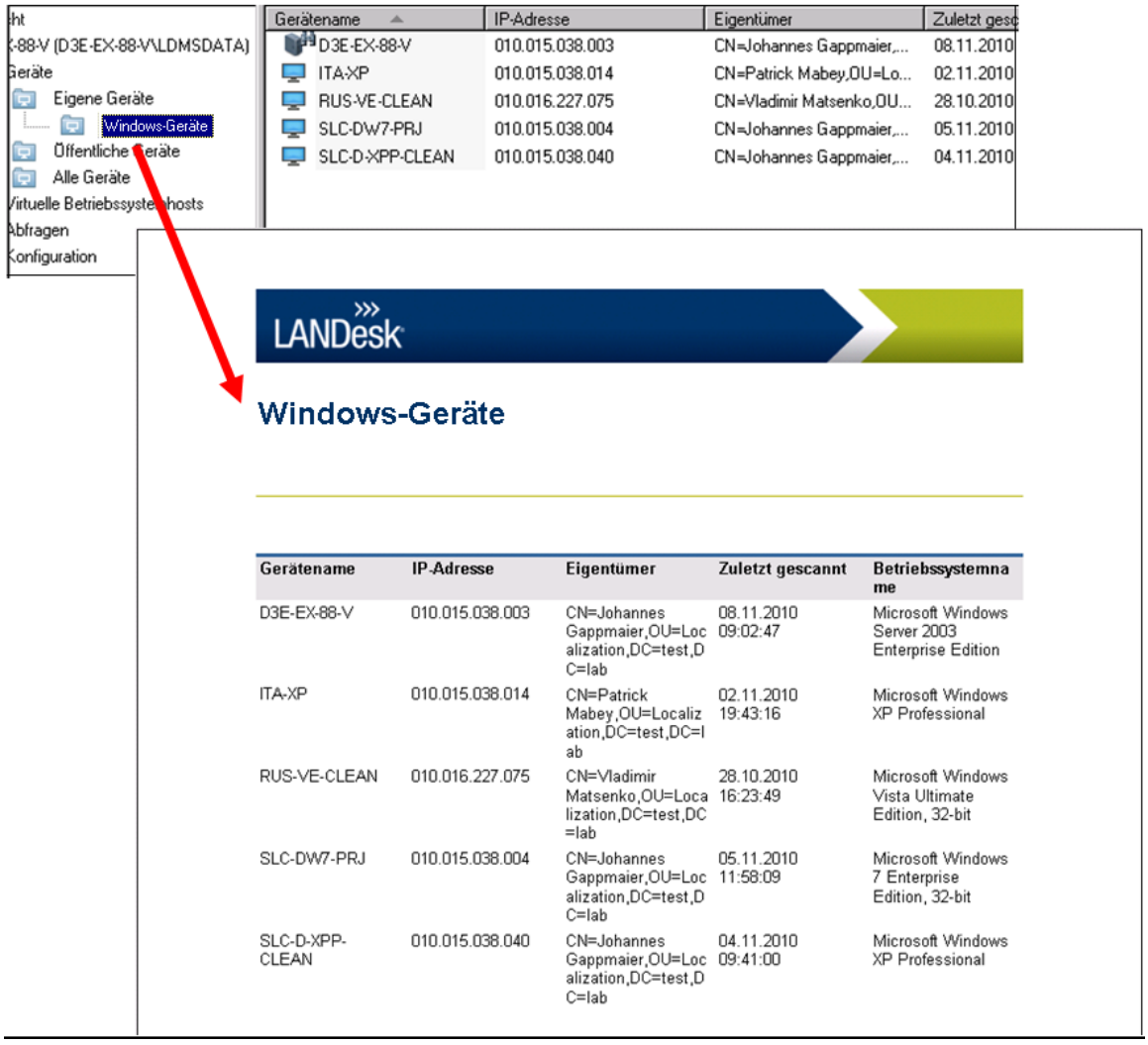
3. Nehmen Sie die gewünschten Änderungen im Berichtsdesigner vor. Klicken Sie, nachdem Sie alle Daten eingegeben haben, in der Symbolleiste auf die Schaltfläche **Speichern**.

Ausführen von Ad-hoc-Berichten

Für die Mehrzahl der Elemente in der Windows-Konsole stehen einfache Berichte zur Verfügung. Jede Gruppe bzw. jeder Container (wie z. B. eine Abfrage) besitzt im Kontextmenü eine Option zum Ausführen eines Berichts. Der Bericht zeigt die Daten in der aktuellen Ansicht an, wobei diese entsprechend den Datenspalten organisiert sind, die in der Konsole angezeigt werden.

Wenn Sie beispielsweise einen Ad-hoc-Bericht mit einem Mausklick von einer Gruppe in der Netzwerkansicht ausführen, zeigt dieser Bericht eine Liste der Geräte in dieser Gruppe. Die Spalten in der Netzwerkansicht (wie beispielsweise "IP-Adresse", "Eigentümer" usw.) werden in dem Bericht angezeigt. Wenn Sie die Gestaltung der Berichtsdaten ändern wollen, ändern Sie den Spaltensatz, bevor Sie den Bericht ausführen (indem Sie Spalten hinzufügen bzw. daraus entfernen oder deren Reihenfolge ändern).

Sie können für viele Extras Berichte ausführen, die Elemente in einer bestimmten Ansicht zeigen (wie z. B. eine Liste der Alarmregelsätze im Extra "Alarmierung".) Sie können für jede Abfrage und jede beliebige Gruppe, die Sie in der Netzwerkansicht oder an anderer Stelle erstellt haben, einen Bericht ausführen.



Berichte können auf dreierlei Wegen schnell und einfach von der Konsole aus erstellt werden:

- **Als Bericht anzeigen:** Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie diese Option, um die Daten in einem Standardberichtsformat anzuzeigen. Ein Vorschaufenster für den Bericht wird geöffnet und Sie können verschiedene Optionen auswählen, bevor Sie den Bericht drucken, speichern oder versenden.
- **Als CSV-Datei exportieren:** Klicken Sie mit der rechten Maustaste auf ein Element und wählen Sie diese Option, um die Daten in einer Wertedatei mit Trennkommas zu speichern.

- **Neuer Bericht:** Klicken Sie mit der rechten Maustaste auf eine Abfrage und wählen Sie diese Option, um einen neuen Bericht auf der Basis der Abfrage zu erstellen. Sie können ein Standardformat verwenden oder den Berichtsdesigner aufrufen, um den Bericht Ihren Vorstellungen entsprechend anzupassen. Der neue Bericht wird im Ordner "Eigene Berichte" gespeichert.

Ausführen eines Ad-hoc-Berichts

Für die Mehrzahl der Elemente in der Windows-Konsole stehen einfache Berichte zur Verfügung. Jede Gruppe bzw. jeder Container (wie z. B. eine Abfrage) besitzt im Kontextmenü eine Option zum Ausführen eines Berichts. Der Bericht zeigt die Daten in der aktuellen Ansicht an, wobei diese entsprechend den Datenspalten organisiert sind, die in der Konsole angezeigt werden.

1. Klicken Sie in der Windows-Konsole mit der rechten Maustaste auf ein Baumelement, wie beispielsweise eine Gruppe in der Netzwerkansicht oder ein Element in einem Extrabereich.
2. Wenn es ein Menüelement namens **Als Bericht anzeigen** gibt, klicken Sie darauf und klicken dann auf das gewünschte Berichtsformat.

Wenn es kein Menüelement namens **Als Bericht anzeigen** gibt, dann bietet das von Ihnen mit der rechten Maustaste angeklickte Element keine Unterstützung für diese Option.

Speichern eines Berichts als CSV-Datei

Sie können Daten zu den meisten Elementen in der Windows-Konsole als CSV-Datei (d. h. als Datei mit kommabegrenzten Werten) speichern. Elemente mit diesem Merkmal weisen im Kontextmenü eine Option auf, mit der die Berichtsdaten in diesem Format gespeichert werden.

1. Klicken Sie in der Windows-Konsole mit der rechten Maustaste auf ein Baumelement, wie beispielsweise eine Gruppe in der Netzwerkansicht oder ein Element in einem Extrabereich.
2. Wählen Sie **Als CSV-Datei exportieren** aus und geben Sie den gewünschten Speicherort für die CSV-Datei an.

Wenn es kein Menüelement namens **Als CSV-Datei exportieren** gibt, dann bietet das von Ihnen mit der rechten Maustaste angeklickte Element keine Unterstützung für diese Option.

Erstellen eines Berichts aus einer Abfrage

Sie können für jede Abfrage und jede Gruppe, die Sie in der Netzwerkansicht oder an anderer Stelle erstellt haben, einen Bericht ausführen.

1. Klicken Sie mit der rechten Maustaste auf eine Abfrage in der Netzwerkansicht.
2. Wählen Sie das Menüelement **Neuer Bericht** aus.
3. Geben Sie einen Namen und eine Beschreibung für den Bericht ein und nehmen Sie alle weiteren von Ihnen gewünschten Änderungen vor.
4. Klicken Sie auf **OK**, um den Bericht zu speichern.

Wenn es kein Menüelement namens **Neuer Bericht** gibt, dann bietet das von Ihnen mit der rechten Maustaste angeklickte Element keine Unterstützung für diese Option.

Organisieren von Berichten

Wenn Sie die Standardberichte verwenden und benutzerdefinierte Berichte erstellen, werden Sie diese sicher auch Ihren Anforderungen entsprechend organisieren und ändern wollen.

Kopieren und Ändern

Standardberichte können nicht gelöscht, aber mit Kopieren und Einfügen in andere Ordner kopiert werden. Sie könnten beispielsweise einen Ordner unterhalb des Ordners **Eigene Berichte** erstellen, der die von Ihnen am häufigsten verwendeten Berichte enthält.

Sie können auch einen Standardbericht kopieren, ihn bearbeiten und als spezifischen Bericht speichern. Dies ist in der Regel einfacher, als einen Bericht von Grund auf neu zu erstellen. Jedes Mal, wenn Sie einen Bericht kopieren, wird eine Nummer an den Berichtsnamen angefügt, um diese Kopie von anderen Kopien zu unterscheiden. Wenn Sie einen Bericht bearbeiten, können Sie ihm einen eindeutigen Namen geben.

HINWEIS: Für jede von Ihnen erstellte Version sollten Sie eine separate Kopie des betreffenden Berichts erstellen. Wenn Sie einen Bericht kopiert und geändert haben und dann zusätzliche Änderungen vornehmen und ihn erneut speichern, gehen Ihre zuvor vorgenommenen Änderungen verloren. Daher empfiehlt es sich, jedes Mal eine neue Kopie anzulegen, damit sichergestellt ist, dass keine Abfragen oder Parameter verloren gehen.

Freigabe für andere Coreserver

Berichte werden unter Rückgriff auf die Datenbank eines Coreservers ausgeführt. Wenn Sie mehrere Coreserver besitzen, können Sie Berichte zur gemeinsamen Nutzung freigeben, so dass die Berichterstellung in Ihrer Organisation standardisiert erfolgt.

Mit der Option **Auf anderen Core bzw. andere Cores** kopieren können Sie einen Bericht auch nur ein einziges Mal freigeben. Damit wird eine Kopie eines Berichts in derselben Ordnerstruktur des Berichterstellungstools des anderen Coreservers gespeichert.

Wenn Sie einen Bericht permanent freigeben wollen, können Sie Berichte zwischen Coreservern synchronisieren. Jedes Mal, wenn ein Bericht geändert wird, erfolgt automatisch eine Sicherung einer Kopie des geänderten Berichts auf allen anderen Coreservern, die Sie zur Synchronisierung von Inhalten ausgewählt haben. Diese Funktion ist Teil des Extras **Coresynchronisierung**.

Importieren und Exportieren

Sie können Berichte importieren oder exportieren, um Kopien Ihrer Berichte zu speichern oder um Berichte oder Vorlagen für andere freizugeben. Wenn Sie beispielsweise exportierte Kopien Ihrer Berichte gespeichert haben und einen Bericht gelöscht haben und später beschließen, dass Sie den Bericht doch wieder benötigen, dann können Sie ihn erneut importieren.

Berichte werden als Nur-Text-XML-Dateien mit der Dateinamenerweiterung .ldms an dem von Ihnen angegebenen Speicherort gespeichert. Diese Dateien können nur von LANDesk Management Suite gelesen werden.

Die Ordner- und Dateinamen stimmen in der Regel mit denen überein, die im Extra "Berichte" erscheinen.

Kopieren, Verschieben und Löschen von Berichten

Sie können jeden Bericht kopieren, ihn bearbeiten und als spezifischen Bericht speichern. Dies ist in der Regel einfacher, als einen Bericht von Grund auf neu zu erstellen. Wenn Sie einen Bericht kopieren, wird eine Nummer an den Berichtsnamen angefügt, um diese Kopie von anderen Kopien zu unterscheiden. Wenn Sie einen Bericht bearbeiten, können Sie ihm einen eindeutigen Namen geben.

HINWEIS: Für jede von Ihnen erstellte Version sollten Sie eine separate Kopie des betreffenden Berichts erstellen. Wenn Sie einen Bericht kopiert und geändert haben und dann zusätzliche Änderungen vornehmen und ihn erneut speichern, gehen Ihre zuvor vorgenommenen Änderungen verloren. Daher empfiehlt es sich, jedes Mal eine neue Kopie anzulegen, damit sichergestellt ist, dass keine Abfragen oder Parameter verloren gehen.

So kopieren oder verschieben Sie Berichte

1. Klicken Sie auf **Extras > Berichte / Überwachung > Berichte**.
2. Erweitern Sie die Baumstruktur, um den gewünschten Bericht zu finden.
3. Ziehen Sie den Bericht in einen anderen Ordner.

HINWEIS: Zwar können Sie jede Art von Bericht kopieren, aber nur benutzerdefinierte Berichte oder kopierte Berichte können Sie ausschneiden und kopieren. Hierzu klicken Sie mit der rechten Maustaste auf den Bericht und klicken auf **Ausschneiden**, öffnen Sie dann den Zielordner, klicken Sie mit der rechten Maustaste und wählen Sie **Einfügen** aus.

So löschen Sie einen Bericht

1. Klicken Sie auf **Extras > Berichte / Überwachung > Berichte**.
2. Erweitern Sie die Baumstruktur, um den gewünschten Bericht zu finden.
3. Wählen Sie den Bericht aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen**.

Nur benutzerdefinierte oder kopierte Berichte können gelöscht werden.

Synchronisieren von Berichten zwischen Coreservern

Berichte können zwischen mehreren Coreservern synchronisiert werden. Mit der Coresynchronisierung können Sie Konfigurationen und Tasks manuell oder automatisch von einem Core auf einen anderen Core kopieren. Die Synchronisierung versetzt Sie in die Lage, Elemente in regelmäßigen Abständen zu kopieren und sicherzustellen, dass mehrere Coreserver dieselben Extras und Daten verwenden.

1. Klicken Sie auf **Extras > Administration > Coresynchronisierung**.
2. Klicken Sie unter **Komponenten** mit der rechten Maustaste auf Berichte und wählen Sie **Automatische Synchronisierung**.

Um einen Bericht mit anderen Cores zu synchronisieren, klicken Sie mit der rechten Maustaste auf den Bericht und klicken Sie dann auf **Automatische Synchronisierung**.

Verwandte Themen

"Coresynchronisierung" auf Seite 97

Kopieren von Berichten auf andere Coreserver

Mit der Option **Auf anderen Core bzw. andere Cores kopieren** können Sie einen Bericht bei Bedarf synchronisieren. Hierbei können Sie die Server auswählen, die die Kopie erhalten sollen. Der Kopiervorgang findet nur einmal statt und das kopierte Element steht sofort auf den Remote-Cores zu Verfügung.

1. Blenden Sie im Extra **Berichte** die Baumstruktur ein und wählen Sie einen Bericht zum Kopieren aus. Verwenden Sie Strg + Klick oder Umschalt + Klick zur Auswahl mehrerer Berichte.
2. Klicken Sie mit der rechten Maustaste auf den Bericht und klicken Sie dann auf **Auf anderen Core bzw. andere Cores kopieren**.
3. Wählen Sie die Coreserver aus, die eine Kopie erhalten sollen.
4. Klicken Sie auf **Inhalt kopieren**, um den Kopiervorgang sofort zu starten.

Beachten Sie, dass Sie unter Umständen die Konsolenansicht des Remote-Cores durch Drücken der Taste **F5** aktualisieren müssen, damit das Element angezeigt wird. Die Remotekopien haben denselben Namen und Speicherort wie die Quellkopie und können bearbeitet werden. Gruppen oder Untergruppen, die den Bericht enthalten, werden automatisch erstellt.

Importieren und Exportieren von Berichten

Exportierte Berichte werden als Nur-Text-XML-Dateien mit der Dateinamenerweiterung .ldms an dem von Ihnen angegebenen Speicherort gespeichert. Diese Dateien können nur von LANDesk Management Suite gelesen werden.

Die Ordner- und Dateinamen stimmen in der Regel mit denen überein, die im Extra "Berichte" erscheinen.

So exportieren Sie einen Bericht

1. Blenden Sie im Extra **Berichte** die Baumstruktur ein und wählen Sie einen Bericht zum Exportieren aus.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren**.
3. Navigieren Sie an den Speicherort, an den Sie den Bericht exportieren möchten und klicken Sie auf **Speichern**.

So importieren Sie einen Bericht

1. Wählen Sie im Extra **Berichte** den Ordner aus, in dem Sie die importierten Berichte speichern möchten (Eigene Berichte oder Öffentliche Berichte).
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Importieren**.
3. Navigieren Sie zum Speicherort des Berichts, den Sie importieren möchten und klicken Sie dann auf **Öffnen**.
4. Wählen Sie im Dialogfeld **Importoptionen** eine Importoption aus.
    - **Aktualisieren:** Fügt Berichte zu den in der .ldms-Datei angegebenen Gruppen hinzu und behält die Kennung bei. Sollte der Bericht bereits vorhanden sein, wird er nicht dupliziert.
    - **Elemente in die ausgewählte Gruppe oder den ausgewählten Eigentümer einfügen:** Fügt Berichte zu der von Ihnen ausgewählten Gruppe hinzu, weist eine neue Kennung zu und aktualisiert den Eigentümer. Wenn der Bericht bereits vorhanden ist, wird eine zweite Kopie mit angehängter Versionsnummer gespeichert.

- **Elemente in die in der .ldms-Datei definierten Gruppen einfügen:** Fügt Berichte zu den in der .ldms-Datei angegebenen Gruppen hinzu und weist eine neue Kennung zu. Wenn der Bericht bereits vorhanden ist, wird eine zweite Kopie mit angehängter Versionsnummer gespeichert.

5. Klicken Sie auf die Schaltfläche **Importieren**.

Erstellen von benutzerdefinierten Berichten

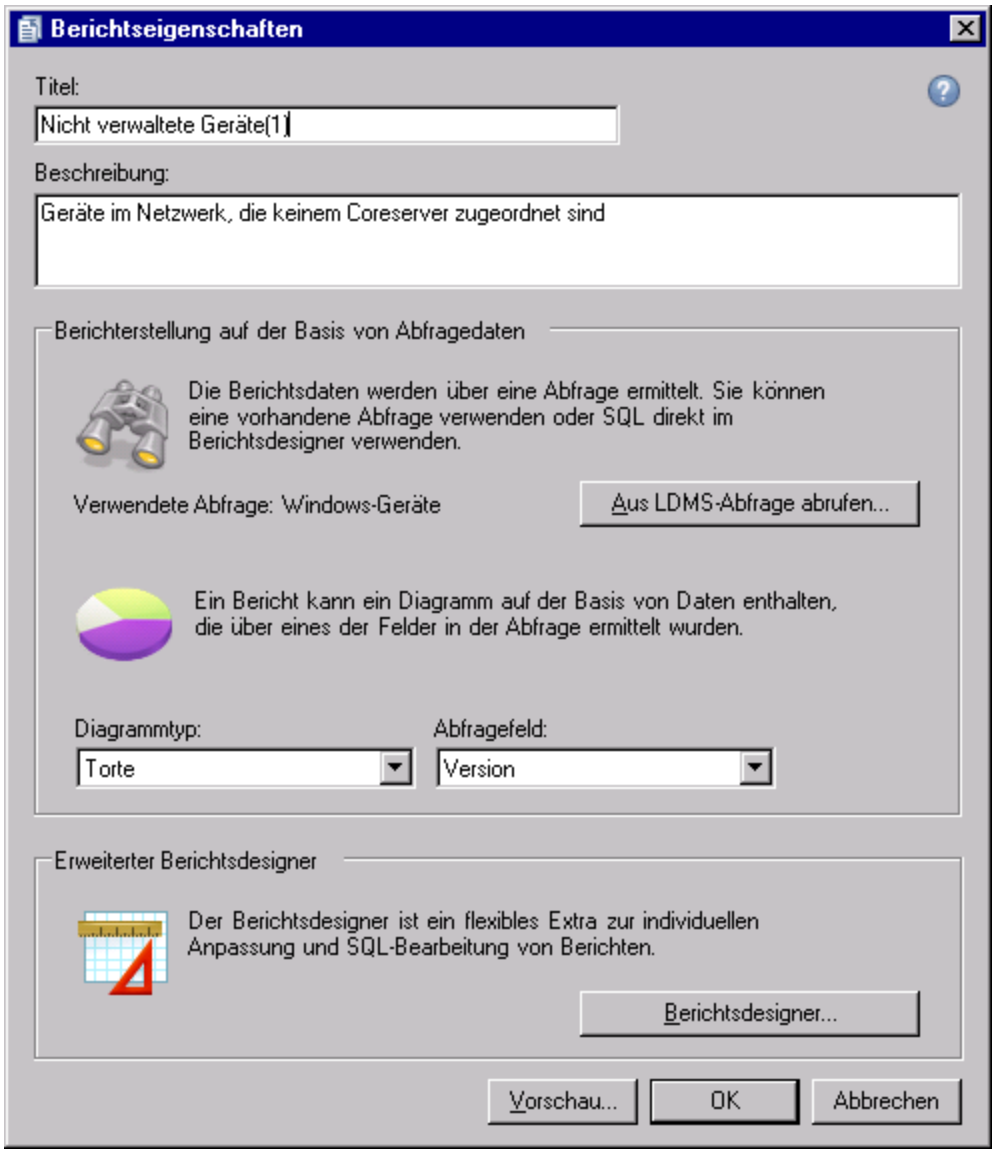
Das Extra "Berichte" verfügt über einen integrierten Data Dynamics-Berichtsdesigner, der Ihnen volle Kontrolle über sämtliche Aspekte von Berichten gibt. Im Designer verwenden Sie Seitenlayoutelemente, die mit Datenobjekten verknüpft sind, um die ausgewählten Daten anzuzeigen. Sie können die Darstellung des Berichts, die zugrunde liegenden SQL-Abfrageanweisungen, die für Benutzer verfügbaren Parameter sowie weitere Merkmale Ihren Anforderungen entsprechend anpassen.

Sie können einen Bericht wie folgt erstellen oder ändern:

- Indem Sie einen Standardbericht kopieren, diesen in "Eigene Berichte" einfügen und dann bearbeiten.
- Indem Sie eine Abfrage in der Management Suite erstellen und diese Abfrage als Basis für den Bericht verwenden.
- Indem Sie einen komplett neuen Bericht unter Verwendung von Datenquellen, Parametern, SQL-Anweisungen, Seitenlayoutelementen und Bildern erstellen.

Berichtseigenschaften

Wenn Sie einen Bericht erstellen oder bearbeiten, legen Sie zunächst die Berichtseigenschaften fest.


Berichtseigenschaften
Titel:
Nicht verwaltete Geräte(1
Beschreibung:
Geräte im Netzwerk, die keinem Coreserver zugeordnet sind
Berichterstellung auf der Basis von Abfragedaten
Die Berichtsdaten werden über eine Abfrage ermittelt. Sie können eine vorhandene Abfrage verwenden oder SQL direkt im Berichtsdesigner verwenden.
Verwendete Abfrage: Windows-Geräte
Aus LDMS-Abfrage abrufen...
Ein Bericht kann ein Diagramm auf der Basis von Daten enthalten, die über eines der Felder in der Abfrage ermittelt wurden.
Diagrammtyp:
Torte
Abfragefeld:
Version
Erweiterter Berichtsdesigner
Der Berichtsdesigner ist ein flexibles Extra zur individuellen Anpassung und SQL-Bearbeitung von Berichten.
Berichtsdesigner...
Vorschau...
OK
Abbrechen

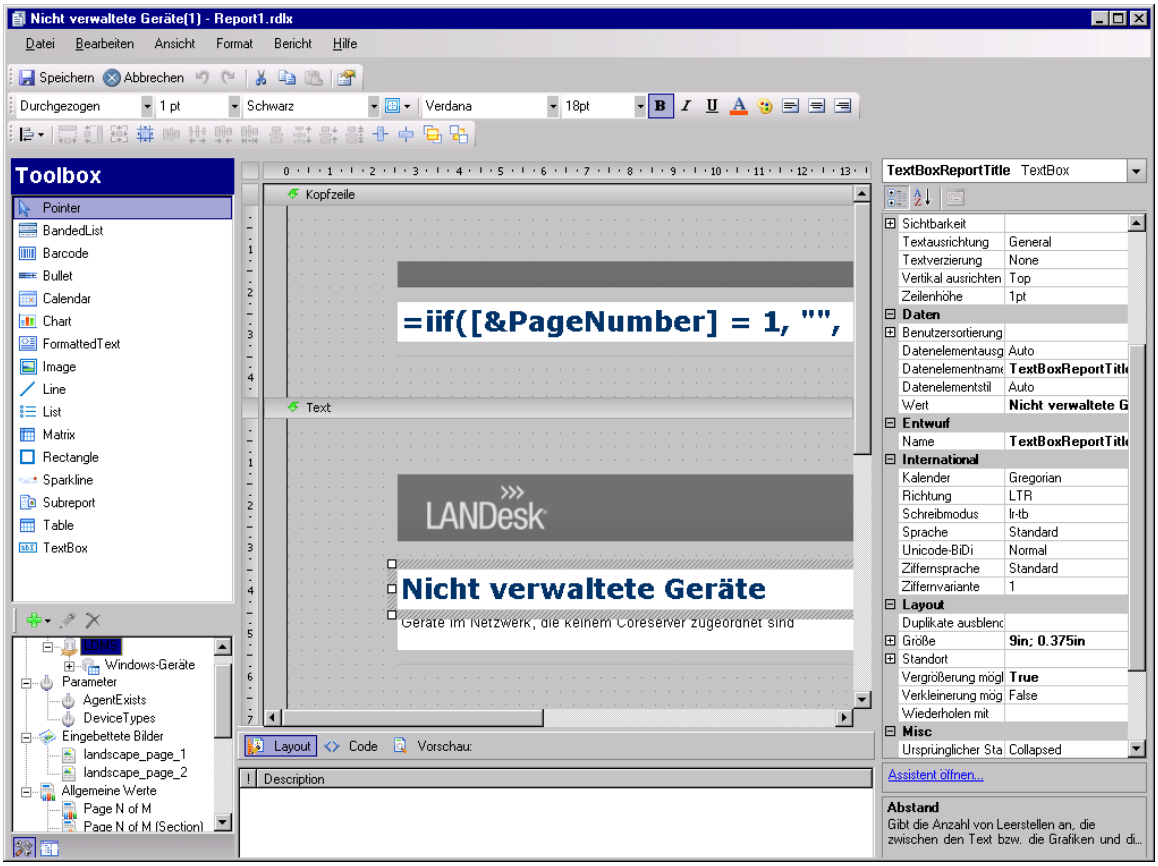
- **Titel:** Geben Sie einen aussagekräftigen Titel für den Bericht ein.
- **Beschreibung:** Fügen Sie zusätzliche beschreibende Informationen zum Bericht hinzu.
- **Aus LDMS-Abfrage abrufen:** Wählen Sie eine Management Suite-Abfrage aus und verwenden Sie diese als Basis für einen neuen Bericht.
- **Diagrammtyp:** Wählen Sie einen Diagrammtyp (Torten- oder Balkendiagramm) aus.
- **Abfragefeld:** Geben Sie an, welches Feld aus dem Bericht im Diagramm dargestellt werden soll.
- **Berichtsdesigner** Öffnen Sie die Berichtsdesigner-Anwendung, um einzelne Änderungen an den Berichtsdaten und dem Layout vorzunehmen. (Sollte diese Schaltfläche abgeblendet dargestellt sein, verfügt der Benutzer nicht über entsprechende Rechte für den Berichtsdesigner.)
- **Vorschau:** Zeigt den Bericht mit den von Ihnen in diesem Dialogfeld ausgewählten Optionen an.

Wenn Sie einen Standardbericht kopiert haben, können Sie Elemente einfach im Dialogfeld "Eigenschaften" ändern und den neuen Bericht speichern. Sollten wesentliche Änderungen erforderlich sein, werden Sie aber vermutlich doch den Berichtsdesigner aufrufen.

Berichtsdesigner

Der Berichtsdesigner kann vom Dialogfeld "Berichtseigenschaften" aus aufgerufen werden. Hierbei handelt es sich um eine eigenständige Anwendung namens Data Dynamics Reports, die im Extra "Berichte" und in die Datenbank integriert ist.

HINWEIS: Um den Berichtsdesigner öffnen zu können, muss ein Benutzer das Recht "Berichtsdesigner - Bearbeiten" besitzen.



Der Berichtsdesigner gewährt vollen Zugriff auf alle Aspekte eines Berichts.

- **Seitenlayout:** In der Mitte des Designers wird das Seitendesign des Berichts angezeigt. Klicken Sie auf die Schaltfläche **Vorschau** unterhalb des Layouts, um den Bericht-Viewer aufzurufen und zu sehen, wie der Bericht bei seiner Ausführung aussehen würde.
- **Toolbox:** Ziehen Sie ein Tool auf das Seitenlayout, um das entsprechende Objekt zu platzieren.
- **Dokumentgliederung:** Zeigt eine Gliederung des Berichtsinhalts in der linken Spalte (anstelle der Toolbox) an.
- **Datenquellen:** Geben Sie hier die Datenquellen an, die Sie bei der Ausführung des Berichts verwenden möchten. Definieren Sie die Quelle für die Daten und fügen Sie anschließend Datasets (Abfragen) und Parameter hinzu, die Sie im Bericht verwenden werden.
- **Parameter:** Hier definieren Sie die Parameter, die die Berichtsergebnisse bestimmen.

- **Eigenschaften:** In der rechten Spalte werden die Eigenschaften angezeigt, die beim ausgewählten Objekt bearbeitet werden können.
- **Assistent:** Klicken Sie auf **Assistent öffnen**, um alle Eigenschaften für das ausgewählte Objekt nach Optionstyp geordnet anzuzeigen.

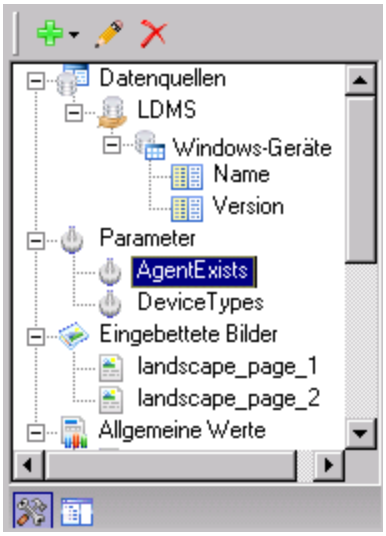
Grundlagen der Erstellung und Bearbeitung von Berichten

Der Berichtsdesigner ist ein flexibles Extra mit vielfältigen Funktionen, die Ihnen die Abfrage und Anzeige von Daten aus einer Vielzahl von unterschiedlichen Quellen ermöglichen. Zur Erstellung eines Berichts sind folgende Grundelemente erforderlich:

- Eine Datenquelle und definierte Datasets, mit denen der Bericht aufgefüllt wird.
- Ein Seitenlayout für die visuelle Darstellung der Daten.
- Datenbereiche und andere Berichtselemente zur Formatierung der Daten.

Datenquellen und Datasets

Berichte extrahieren Informationen aus der *Datenquelle*, einer Datenbank, die ein Standardformat wie SQL, ODBC, Oracle oder XML verwendet. In Verbindung mit der Datenquelle definieren Sie *Datasets*, d. h. Abfragen, auf die der Bericht Bezug nimmt. Der Daten-Explorer auf der linken Seite des Designers zeigt Datenquellen und Datasets in einer Baumstruktur an. Im nachstehenden Beispiel ist "LDMS" die Datenquelle (die Datenbank der Management Suite) und "Windows-Geräte" ist ein Dataset. "Name" und "Version" sind Namen von Feldern (Datenbanktabellen) die in der Dataset-Abfrage referenziert werden.

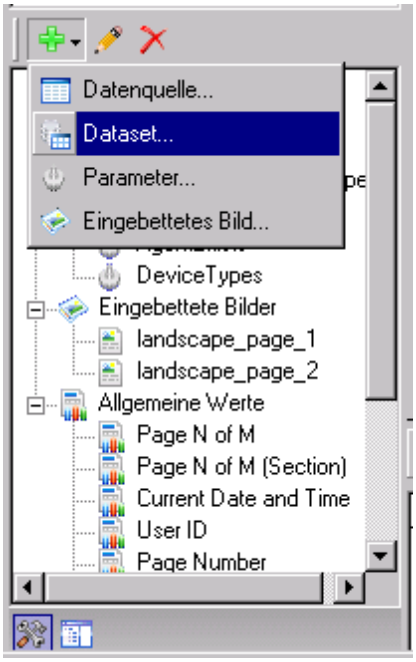


Wenn Sie einen neuen Bericht erstellen, wird standardmäßig die Management Suite-Datenbank als Standarddatenquelle anzeigt. Sie können eine beliebige andere Quelle hinzufügen, indem Sie einen Datentyp, eine Verbindungszeichenfolge sowie eventuell erforderliche Anmeldeinformationen für den Zugriff auf die Daten angeben. Damit können Sie zur Erstellung von benutzerdefinierten Berichten nicht nur aus der Management Suite-Datenbank Daten extrahieren, sondern auch aus jeder anderen Datenquelle.

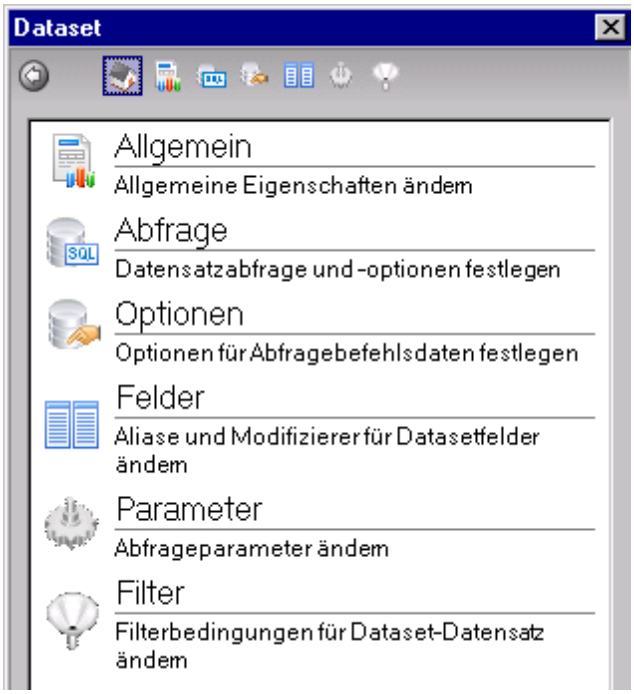
Parameter dienen der Übergabe von Informationen zwischen Datasets. Im Bericht-Viewer können Parameter angezeigt werden, die es dem Benutzer gestatten, die Auswahl der angezeigten Daten einzuschränken.

Hinzufügen von Datenelementen

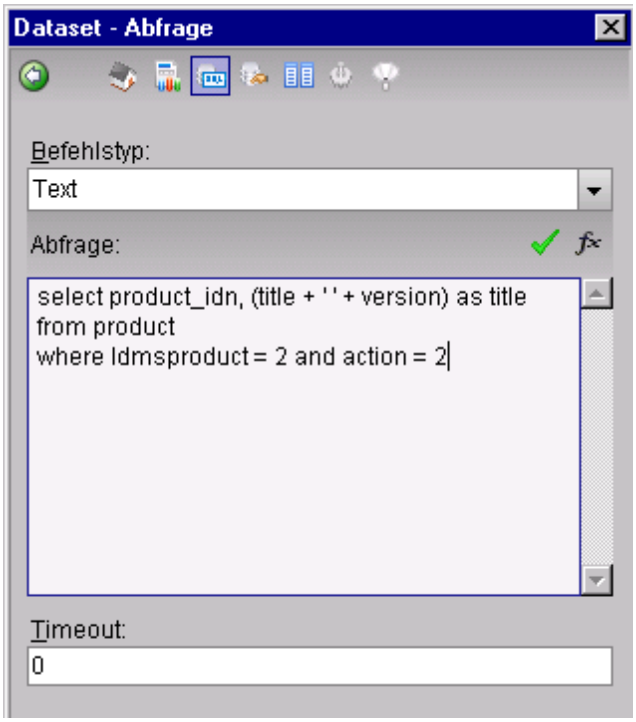
Der Berichtsdesigner bietet Assistenten, die Ihnen bei der Herstellung von Verknüpfungen zu Datenquellen, der Definition von Datasets und Parametern Hilfestellung geben. Beispiel: Sie klicken zunächst auf eine Datenquelle (wie z. B. LDMS), klicken dann auf die Schaltfläche **Hinzufügen** und wählen **Dataset** aus.



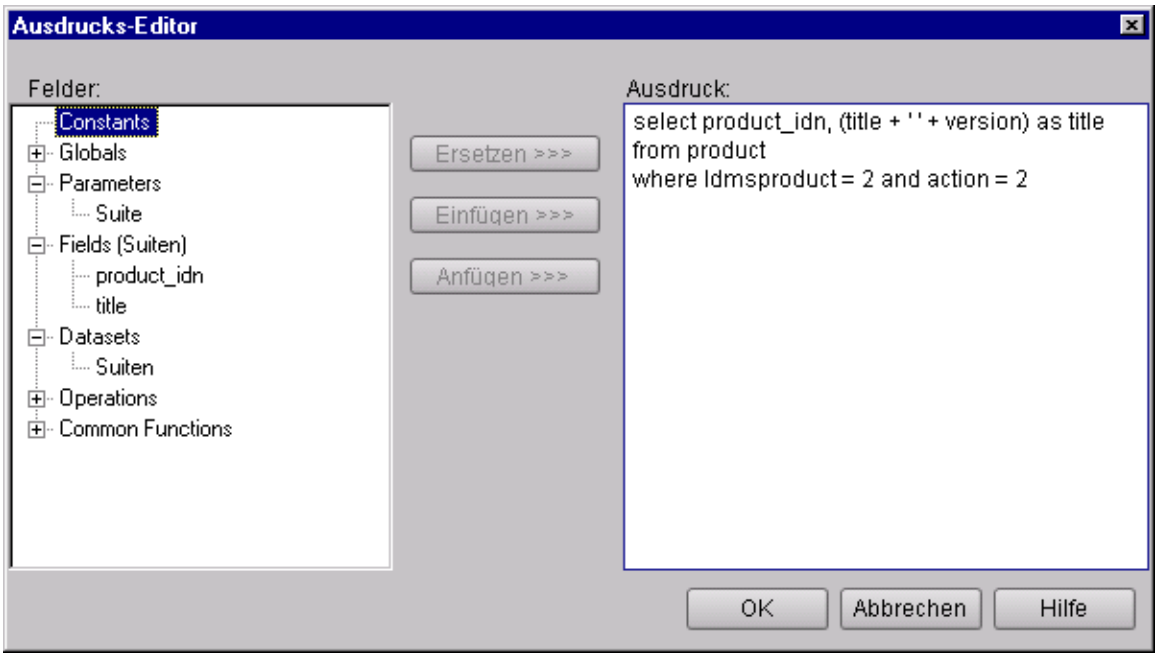
Daraufhin erscheint der Dataset-Assistent und zeigt sechs Gruppen mit Eigenschaften an.



Auf der Seite "Abfrage" des Assistenten können Sie beispielsweise eine SQL-Abfrage hinzufügen. Klicken Sie auf das grüne Häkchen, um die Syntax zu prüfen, und klicken Sie auf das Funktionssymbol (*fx*), um den Ausdrucks-Editor zu öffnen.

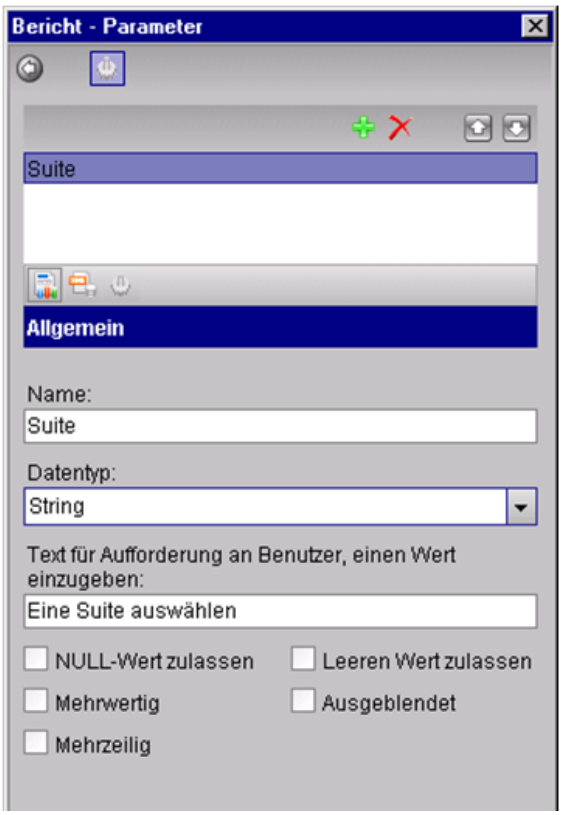


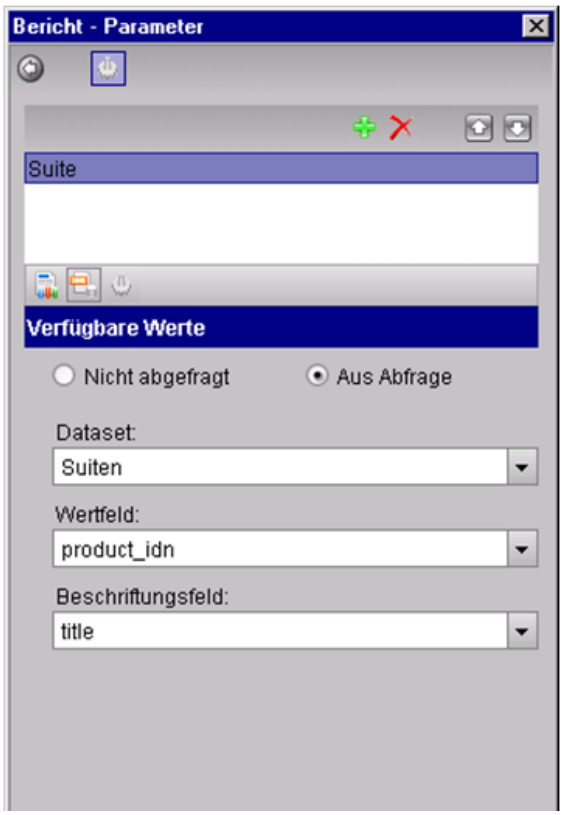
Der Ausdrucks-Editor listet alle Felder, die für das ausgewählte Element verfügbar sind und gibt Ihnen die Möglichkeit, diese Elemente, wie z. B. Parameter und Felder aus Datasets, in einen Ausdruck einzufügen. Abgesehen von den Feldern, die sich auf Ihre Datasets beziehen, gibt es häufig verwendete Werte, die global definiert sind, sowie Standardoperatoren und -funktionen, die Sie in einen Ausdruck einfügen können.



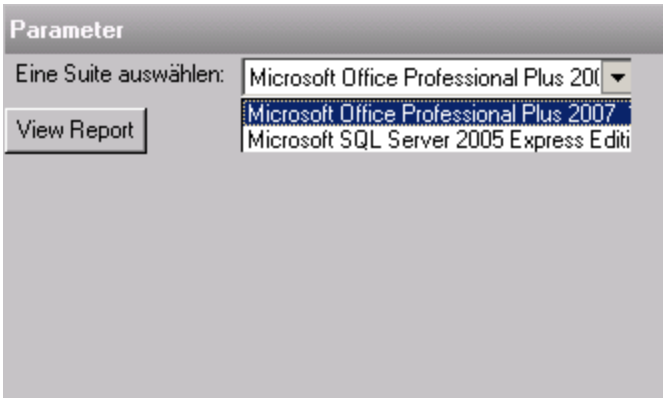
Nachdem Sie mindestens ein Dataset hinzugefügt haben, können Sie Parameter auf der Basis Ihrer Datasets hinzufügen. Wenn ein Benutzer einen Bericht ausführt, werden die von Ihnen hinzugefügten Parameter im Bericht-Viewer angezeigt, damit der Benutzer wählen kann, welche Daten im Bericht angezeigt werden.

Im folgenden Beispiel wurde ein Dataset mit dem Namen **Suiten** erstellt, das auf die Tabelle **Produkt** mit den Feldern **product_idn**, **title** und **version** verweist. Ein Parameter mit dem Namen **Suite** wird erstellt. Auf der Seite **Allgemein** des Dialogfelds wird der Name hinzugefügt und ein Text für die Eingabeaufforderung an den Benutzer ("Eine Suite auswählen"). Dies ist die Eingabeaufforderung, die die Benutzer im Bericht-Viewer sehen. Auf der Seite **Verfügbare Werte** werden Werte aus der Abfrage festgelegt. Das Wertfeld ist **product_idn** (eine eindeutige Identifikationsnummer aus der Datenbank) und das Beschriftungsfeld ist **title**, d. h. der Titel (Name) der Suite, der für den Benutzer angezeigt wird.





Wenn der Bericht ausgeführt wird, erscheint dieser Parameter für den Benutzer in Form einer Liste, in der eine Produktsuite ausgewählt werden kann.



Auf der dritten Seite des Dialogfelds "Parameter" können Sie eine Standardauswahl für den Parameter definieren.

Darstellung von Parameterauswahlen in einer Abfrage

Wenn Sie Benutzern die Auswahl eines Parameters gestatten, können Sie auf diese Auswahl in einer Abfrage verweisen, indem Sie eine SQL-Anweisung verwenden, die einzigartig für den Data Dynamics-Berichteditor ist: "in (?)". Diese Anweisung verwendet den derzeit ausgewählten Parameterwert beim Ausführen des Berichts. Ein Beispiel hierfür ist in dem folgenden Codebeispiel gegeben.

Die folgende Abfrage verwendet Felder aus der Tabelle **Produkt** und der Tabelle **slm_productsuiteref** zur Auswahl von Produkten, die in einer Produktsuite enthalten sind. In diesem Fall wird eine einzigen Produktsuite eingeschlossen, ausgewiesen durch ihre Kennung (615).

```
select p.product_idn, p.title, p.version from slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn = 615
order by p.title
```

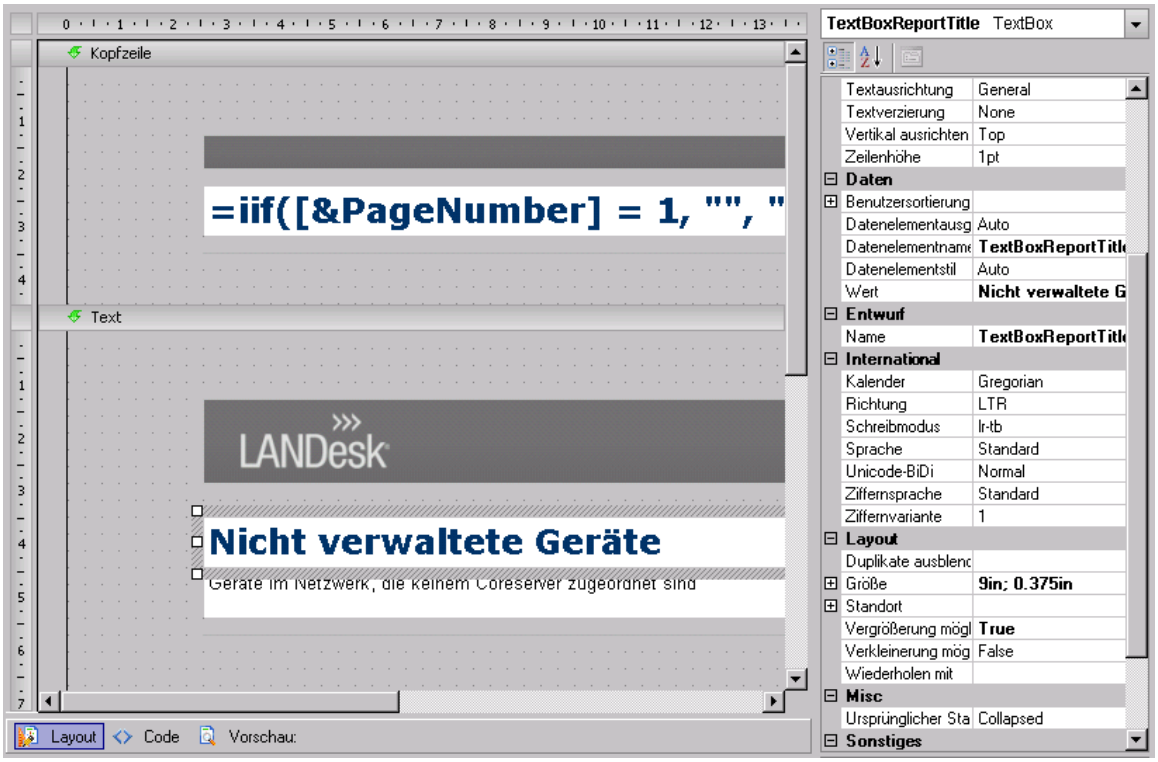
Statt eine bestimmte Suite anzugeben, können Sie die spezifische Produktsuite-Referenz durch "in (?)" ersetzen, um die diejenige Suite einzubeziehen, die der Benutzer beim Ausführen des Berichts auswählt.

```
select p.product_idn, p.title, p.version from slm_productsuiteref r
left outer join product p on p.product_idn = r.product_idn where r.productsuite_idn in (?)
order by p.title
```

Weitere Anwendungsbeispiele finden Sie in einigen Standardberichte, bei denen der Benutzer einen Parameterwert auswählen muss.

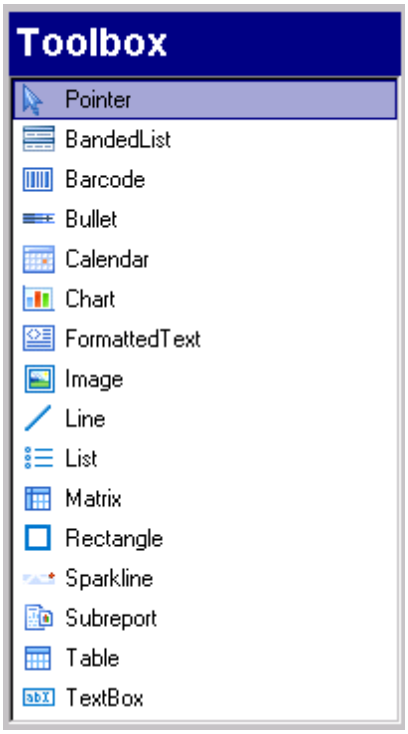
Layout

Berichtslayouts legen die Seitenausgabe unter Verwendung von Standardseitenformaten fest. Sie können die Seitengröße bzw. das Papierformat, die Ausrichtung, eine sich wiederholende Kopf- und Fußzeile und ein Format für den Textkörper des Berichts definieren.



Standardberichte verwenden eine Kopfzeile mit einem LANDesk Logo, das auf der Seite 1 unterdrückt wird. Der Textkörper beginnt mit einem größeren Logo, das nur einmal auftritt und an das sich die Daten auf der für deren Ausgabe erforderlichen Anzahl von Seiten anschließen.

Bei der Bearbeitung des Seitenlayouts können Sie Formatierungsmerkmale und Datenbereichselemente einfach und schnell hinzufügen, indem Sie die entsprechenden Extras aus der Toolbox ziehen.



Ziehen Sie ein Element auf das Layout, verschieben Sie es dann und passen Sie die Größe an. Definieren Sie Objektdetails im Eigenschaftenbereich (auf der rechten Seite des Editors) oder klicken Sie auf **Assistent öffnen**, um dieselben Eigenschaften mit dem Assistenten zu bearbeiten, wobei die Elemente nach Eigenschaftstyp gruppiert werden.

Datenbereiche

Daten werden unter Verwendung von *Datenbereichen* formatiert. Hierbei handelt es sich um Standardformatelemente, die für bestimmte Anzeigetypen definiert sind. Zu den Datenbereichen gehören:

- **Tabelle:** Sie besteht aus Zeilen und Spalten, mit einem Feld aus einen Dataset pro Spalte. Sie können Zeilen auch nach einem Feld gruppieren, beispielsweise wenn Sie Daten nach Gerät gruppieren möchten, wobei es dann für jedes Gerät eine Kopfzeile gibt, unterhalb der dann die unterstützenden Daten stehen. (Ein Beispiel für gruppierte Zeilen finden Sie im Bericht zum Hardwareinventar.)
- **Liste:** In einer Liste wiederholen sich Elemente für jeden Datensatz in der Datenquelle. Sie können jede beliebige Formatierung für Listen verwenden. Für komplexe Gruppierungen können Listen geschachtelt werden, oder eine Liste kann in einen anderen Datenbereich gestellt werden.
- **Vorgruppierte Liste:** Eine Sammlungsgruppe (bestehend aus Kopf-, Detail- und Fußabschnitt) bei der sich Daten im Detailabschnitt gruppiert wiederholen. Vorgruppierte Listen sind praktisch, weil Sie Elemente einfügen können, ohne dass dabei Einschränkungen durch ein bestimmtes Tabellen- oder Listenformat zum Tragen kommen.
- **Matrix:** Sie weist ebenfalls Zeilen und Spalten auf, ist aber mit einem Zeilen- und Spaltenkopf formatiert, wie bei einer Kreuztabelle oder einer Pivottabelle.

Datenregionen sind in der Toolbox enthalten. Sie können kombiniert, geschachtelt und in andere Layout-Elemente eingeschlossen werden.

Berichtselemente

Die Elemente in der Toolbox werden für die Formatierung des Seitenlayouts und die Anordnung der Daten auf der Seite verwendet.

- **Linien** dienen der visuellen Formatierung.
- **Rechtecke** sind visuelle Elemente, die andere Elemente enthalten.
- **Textfelder** können dazu verwendet werden, statischen Text oder dynamische Daten an einer beliebigen Position auf der Seite anzuordnen.
- **Bilder** können an einer beliebigen Position auf der Seite platziert werden.
- **Diagramme** bieten eine Übersicht über ausgewählte Daten.
- **Barcodes** können Daten in 23 Barcodestilen wiedergeben.
- **Sparklines** sind kleine Diagramme, die Daten zusammenfassen und inline in einen Text eingefügt werden können.
- **Kalender** können zu einer Seite hinzugefügt und mit Daten verknüpft werden, so dass Ereignisse innerhalb eines Datumsbereichs angezeigt werden.

Diese und andere Elemente können vollständig vom Benutzer angepasst und auf vielerlei Weise zur Gruppierung und Anzeige von Daten kombiniert werden.

Anregungen für Ihre eigenen Berichte erhalten Sie, wenn Sie die Eigenschaften eines beliebigen Standardberichts anzeigen und auf **Berichtsdesigner** klicken, um so herauszufinden, wie der Bericht definiert wurde.

Zusätzliche Hilfe

Ausführlichere Hilfestellungen zum Berichtsdesigner finden Sie auf der LANDesk User Community-Website (community.landesk.com). Weitere Informationen finden Sie ferner auf der Data Dynamics Reports-Website (datadynamics.com).

Verwenden von Berichten [Webkonsole]

Wenn Sie die Webkonsole verwenden, stehen Ihnen alle Berichte der Windows-Konsole zur Verfügung, wobei jedoch geringfügige Unterschiede in der Art und Weise bestehen, in der Parameter angezeigt und ausgewählt werden. Sie können in der Webkonsole keine benutzerdefinierten Berichte bearbeiten oder erstellen oder Berichte zwischen Ordnern verschieben, wohl aber Berichte anzeigen, drucken und exportieren.

Wenn ein Benutzer einen Bericht von der Webkonsole ausführt, kommt der Bereich des Benutzers für den Bericht zur Anwendung. Der Bericht enthält somit nur Daten von Geräten innerhalb des Bereichs des Benutzers.

Um Berichte in der Webkonsole verwenden zu können, muss ein Benutzer über das Recht zum Anzeigen von Berichten verfügen.

So führen Sie einen Bericht von der Webkonsole aus

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Berichte**.
2. Erweitern Sie die Ordnerstruktur, um den Bericht zu finden, den Sie ausführen möchten.

3. Klicken Sie auf den Bericht.

   Der Bericht wird in einem neuen Browser-Fenster im Bericht-Viewer geöffnet.

4. Wählen Sie die gewünschten Parameter aus und klicken Sie auf **Bericht anzeigen**.
5. Wenn Sie Details zu einem bestimmten Bereich eines Diagramms anzeigen möchten, klicken Sie auf den betreffenden Bereich im Diagramm. In der Ansicht wird daraufhin der Abschnitt des Berichts angezeigt, der die von Ihnen gewünschten Daten enthält.
6. Die Schaltflächen in der Symbolleiste verwenden Sie für die Suche nach Daten, den Export von Daten in ein anderes Format, das Drucken des Berichts usw.
7. Wenn Sie fertig sind, schließen Sie das Vorschau-Browserfenster.

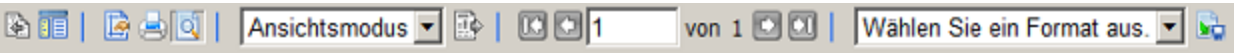
So speichern Sie einen Bericht in der Webkonsole

1. Führen Sie einen Bericht aus.
2. Wählen Sie in der Symbolleiste des Viewers das Berichtsformat, das Sie verwenden wollen, in der Liste **Wählen Sie ein Format aus** und klicken Sie dann auf die Schaltfläche **Exportieren**.
3. Speichern Sie die Datei unter Verwendung der Einstellungen für Ihren Browser.

HINWEIS: Wenn Sie einen Bericht speichern und planen, diesen per E-Mail zu versenden, sollten Sie anstelle der HTML-Ausgabe vorzugsweise das PDF-Format verwenden.

Der Bericht-Viewer der Webkonsole

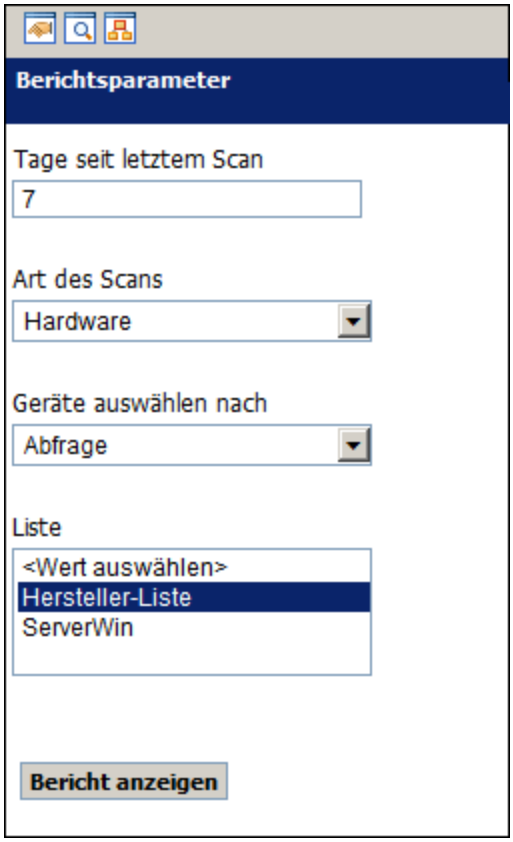
Mit dem Bericht-Viewer der Webkonsole können Sie Berichte anzeigen, drucken und exportieren. Die Symbolleiste umfasst die folgenden Schaltflächen:



- **Zurück zum übergeordneten Bericht:** Wenn Sie gerade einen untergeordneten Bericht anzeigen, kehren Sie hiermit zum übergeordneten Bericht zurück, von dem aus der Unterbericht abgerufen wurde.
- **Randleiste ausblenden/einblenden:** Dient zur Umschaltung des Randleistenbereichs, in dem Such- und Parameteroptionen und eine Dokumentstrukturansicht angezeigt werden.
- **Seiteneinrichtung:** Dient zur Änderung der Einstellungen für Seite, Ausrichtung und Ränder.
- **Drucken:** Öffnet das mit dem von Ihnen gewählten Ausgabetyp verknüpfte Dialogfeld **Drucken**.
- **Druckvorschau:** Dient zum Umschalten der Druckvorschau (Seitenansicht). Ist diese Schaltfläche nicht aktiviert, wird der Bericht als einzelne HTML-Seite angezeigt.
- **Ansichtsmodus:** Anzeige des Berichts im HTML- oder PDF-Format. Wählen Sie ein Format aus der Liste aus und klicken Sie auf die Schaltfläche **Ansichtsmodus**, um das Format zu ändern.
- **Gehe zur ersten Seite:** Hiermit zeigen Sie die erste Seite des Berichts an.
- **Zurück:** Hiermit zeigen Sie die vorherige Seite des Berichts an.
- **Seitenfeld:** Hiermit fügen Sie eine bestimmte Seitenzahl ein, mit der Sie direkt zu der betreffenden Seite gelangen.
- **Weiter:** Hiermit zeigen Sie die nächste Seite in der Seitenabfolge an.
- **Gehe zur letzten Seite:** Hiermit zeigen Sie die letzte Seite des Berichts an.

- **Wählen Sie ein Format aus:** Wählen Sie das Format aus, in dem Sie den Bericht speichern möchten (als PDF-, HTML-, DOC-, XML- oder XLS-Datei)
- **Exportieren:** Hiermit speichern Sie den Bericht in dem von Ihnen gewählten Format.

Die Randleiste bietet drei Optionen, die durch Symbole dargestellt sind. Der Bericht wird im Viewer entsprechend den von Ihnen gewählten Optionen und den jeweiligen Parametern aktualisiert.



- **Parameter:** Hiermit ändern Sie die Parameter des Berichts. Diese können von Bericht zu Bericht variieren. Sobald Sie andere Parameter ausgewählt haben, klicken Sie auf **Bericht anzeigen**, um den Bericht mit den neuen Parametern zu aktualisieren.
- **Suchen:** Sucht nach einer Zeichenfolge in den Berichtsergebnissen. Geben Sie die Zeichenfolge ein und wählen Sie ein beliebiges Kriterium aus (wie z. B. Groß-/Kleinschreibung beachten) und klicken Sie auf **Suchen**. Daraufhin wird eine Liste mit den Vorkommen der Zeichenfolge angezeigt. Klicken Sie auf ein Vorkommen, um zum entsprechenden Abschnitt des Berichts zu gelangen. Das Auftreten der entsprechende Zeichenfolge wird hervorgehoben dargestellt.
- **Dokumentstruktur:** Zeigt eine inhaltliche Gliederung des Berichts, wenn eine Dokumentstruktur für den Bericht definiert wurde. Diese Option wird nicht angezeigt, wenn es keine Dokumentstruktur gibt. Klicken Sie auf ein Element in der Liste, um an die entsprechende Stelle im Bericht zu gelangen.

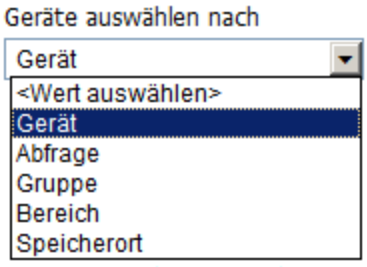
Auswählen von Parametern aus einer Liste

Wenn die Randleiste eine Liste mit Parametern enthält, können Sie alle Listenelemente in den Bericht einbeziehen, indem Sie **(Alle)** auswählen. Wenn Sie dies tun, werden die einzelnen Elemente in der Liste zwar nicht markiert, aber dennoch werden sie alle in den Bericht eingeschlossen.

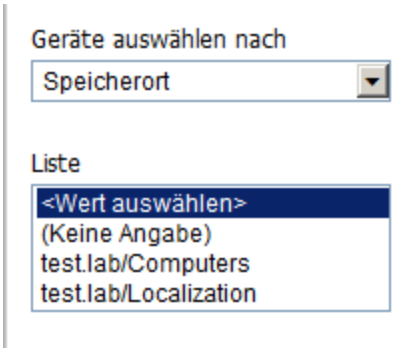
Um eine Untergruppe der Elemente auszuwählen, wählen Sie alle Elemente einzeln aus, die im Bericht enthalten sein sollen. Vergewissern Sie sich, dass **(Alle)** nicht ausgewählt ist. Verwenden Sie Strg + Klick oder Umschalt + Klick zur Auswahl mehrerer Elemente und klicken Sie dann auf **Bericht anzeigen**.

Auswählen von Geräten, Gruppen oder Standorten

Die Parameter variieren je nach Bericht. Alle Berichte enthalten aber eine Option zur Geräteauswahl, mit der einzelne Geräte, Abfragen, Gruppen, der Bereich oder Standort festgelegt wird. Auf diese Weise können Sie einen Bericht für eine Abfrage, eine Gruppe oder einen Bereich generieren, die bzw. den Sie in der Netzwerkansicht definiert haben, oder aber für einen Standort innerhalb Ihres Netzwerks.



So können Sie beispielsweise Geräte an einem Standort anhand des Gerätenetzwerkstandorts auswählen. Wenn Sie "Standort" auswählen, werden in der Liste Standorte in Ihrem Netzwerk nach Domänenname geordnet angezeigt.



Informationen zum Dialogfeld "Task planen"

Bei der Planung eines Berichts können die folgenden Elemente konfiguriert werden. Einige Elemente dienen nur der Information und sind nicht konfigurierbar.

Registerkarte "Übersicht"

- **Eigentümer:** Der Bereich des Berichts entspricht dem Bereich des Benutzers, der den Bericht ausführt. Wenn Sie zu einem anderen Benutzer wechseln möchten, wählen Sie den Benutzer aus der Liste aus.

Registerkarte "Task planen"

- **Ungeplant lassen:** Fügt den Task zum Fenster "Geplante Tasks" hinzu, plant jedoch den Task nicht. Verwenden Sie diese Option, wenn Sie eine Taskkonfiguration zwar speichern, aber nicht ausführen möchten.
- **Jetzt starten:** Der Task wird gestartet, sobald Sie das Dialogfeld geschlossen haben. Der Start des Tasks kann sich um bis zu eine Minute verzögern.
- **Später starten:** Der Task wird zum angegebenen Datum und zur entsprechenden Uhrzeit gestartet.
- **Datum und Uhrzeit:** Der Task wird zum ausgewählten Datum ausgeführt. Geben Sie das Datum im Format TT/MM/JJ ein, oder öffnen Sie die Liste **Datum**, um ein Datum aus dem Kalender auszuwählen.
- **Wiederholen alle:** Der Task wird in regelmäßigen Abständen wieder ausgeführt. Wählen Sie aus der Liste "Tag", "Woche" oder "Monat" aus, um festzulegen, wie häufig der Task ausgeführt werden soll. Er wird zur oben festgelegten Zeit wiederholt.

Registerkarte "Empfänger"

- **LANDesk Berichte-Freigabe** Alle Berichte werden standardmäßig im Ordner ldmain\reports gespeichert, der als Freigabe auf dem Coreserver definiert ist. Jeder Benutzer mit Zugriffsrechten auf diese Freigabe kann den Ordner öffnen und die Berichte anzeigen. Wenn Sie nicht wollen, dass der Bericht in der Freigabe gespeichert wird, deaktivieren Sie dieses Kontrollkästchen.
- **Benutzer:** Aktivieren Sie das Kontrollkästchen für alle Benutzer, die den Bericht erhalten sollen. Damit ein Bericht an einen Benutzer gesendet werden kann, muss in den Eigenschaften des Benutzers eine E-Mail-Adresse angegeben sein. (Dies geschieht mithilfe des Extras **Benutzerverwaltung**.)

Registerkarte "SMTP-Konfiguration"

- **Ausgehender E-Mail-Server (SMTP):** Wählen Sie den SMTP-Server aus, der zum Senden der Berichts-E-Mails verwendet werden soll.
- **Portnummer:** Geben Sie die Portnummer an, die der SMTP-Server verwenden soll.
- **Dieser Server erfordert eine sichere Verbindung (SSL):** Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server eine HTTPS-Verbindung erfordert.
- **Mein Ausgangsserver (SMTP) erfordert Authentifizierung:** Aktivieren Sie dieses Kontrollkästchen, wenn der SMTP-Server Anmeldeinformationen erfordert. Sie können NTLM-Authentifizierung verwenden oder einen Benutzernamen und ein Kennwort angeben.
- **Test-E-Mail:** Geben Sie eine Test-E-Mail-Adresse ein und klicken Sie auf **Testen**, um die SMTP-Einstellungen zu testen und sicherzustellen, dass die SMTP-Konfiguration gültig ist.

Planen von Tasks

Planen von Tasks

LANDesk Management Suite umfasst ein leistungsstarkes System für die Verwaltung geplanter Tasks. Sowohl der Coreserver als auch die verwalteten Geräte verfügen über Dienste/Agenten, die geplante Tasks unterstützen. Management Suite Konsolen und Webkonsolen können Tasks zum Scheduler hinzufügen.

Ein Softwareverteilungstask besteht aus einem Verteilungspaket, einer Verteilungsmethode, Zielgeräten und einem Zeitplan für die Verteilung. Tasks, bei denen es sich nicht um Verteilungstasks handelt, beinhalten ein Skript, Zielgeräte und einen Zeitplan.

Zu den anderen Tasks, die Sie planen können, gehören:

- Gerätekonfigurationen
- Verschiedene benutzerdefinierte Skripts
- Bereitstellen von benutzerdefinierten Datenformularen
- Erkennung nicht verwalteter Geräte
- Anfälligkeitsscans
- Softwareausführung auf verwalteten Geräten

HINWEIS: Konsolenbenutzer, die mit Skripten arbeiten werden, müssen der lokalen Gruppe "LANDesk Script Writers" des Coreservers angehören. Diese Gruppe gibt Konsolenbenutzern Schreibzugriff auf den Order "ManagementSuite\Scripts".

Verwalten von Skripten

LANDesk Management Suite verwendet zum Ausführen von benutzerdefinierten Tasks auf Geräten Skripte. Skripte können im Fenster **Skripte verwalten** (**Extras > Verteilung > Skripte verwalten**) erstellt werden.

Das Fenster "Skripte verwalten" unterteilt Skripte in drei Kategorien:

- **Eigene Skripte:** Skripte, die Sie erstellt haben.
- **Öffentliche Skripte:** Skripte, die die von einem Benutzer mit dem Skriptverwaltungsrecht "Öffentlich bearbeiten" als "Öffentlich" gekennzeichnet wurden. Diese Skripte sind für alle anderen schreibgeschützt. Benutzer können öffentliche Skripte in ihren Ordner **Eigene Skripte** kopieren, um sie zu bearbeiten.
- **Alle Skripte:** Alle Skripte auf dem Coreserver.

Sie können Gruppen unter dem Objekt **Eigene Skripte** erstellen, um Ihre Skripte noch differenzierter zu unterteilen. Um ein neues Skript zu erstellen, klicken mit der rechten Maustaste auf **Eigene Skripte** oder auf eine von Ihnen erstellte Gruppe und klicken dann auf den Skripttyp, den Sie erstellen möchten.

Nachdem Sie ein Skript erstellt haben, können Sie im Kontextmenü des Skripts auf "Planen" klicken. Damit wird das Fenster **Geplante Tasks** geöffnet (**Extras > Verteilung > Geplante Tasks**). In diesem Fenster können Sie angeben, auf welchen Geräten und wann der Task ausgeführt werden soll. Lesen Sie den nachstehenden Abschnitt, um weitere Informationen zum Planen von Tasks zu erhalten.

Aufgrund besonderer Funktionen, die von der Windows-Konsole unterstützt werden, sollten in der Windows-Konsole erstellte Skripte nicht in der Webkonsole bearbeitet werden.

Planen eines Tasks

Im Fenster **Geplante Tasks** können Sie sich über den Status eines geplanten Tasks informieren und nachprüfen, ob Tasks erfolgreich abgeschlossen wurden oder nicht. Der Scheduler-Dienst kann auf zwei Arten mit Geräten kommunizieren:

- Über den Standard LANDesk Agenten (muss bereits auf Geräten installiert sein).
- Über ein Systemkonto auf Domänenebene. Für das Konto, das Sie auswählen, muss die Anmeldung als Dienstprivileg gelten. Weitere Informationen zum Konfigurieren des Scheduler-Kontos finden Sie unter "Konfigurieren des Scheduler-Dienstes" auf Seite 89.

Die Konsole enthält Skripte, die Sie planen können, um routinemäßige Wartungstasks wie die Ausführung von Inventarscans auf ausgewählten Geräten durchzuführen. Sie können diese Skripte von **Extras > Verteilung > Skripte verwalten > Alle anderen Skripte** aus planen.

Damit Sie einen Zeitplan für die Ausführung geplanter Tasks für ein Gerät erstellen können, muss auf dem Gerät der Standard LANDesk Agent installiert und das Gerät in der Inventardatenbank registriert sein.

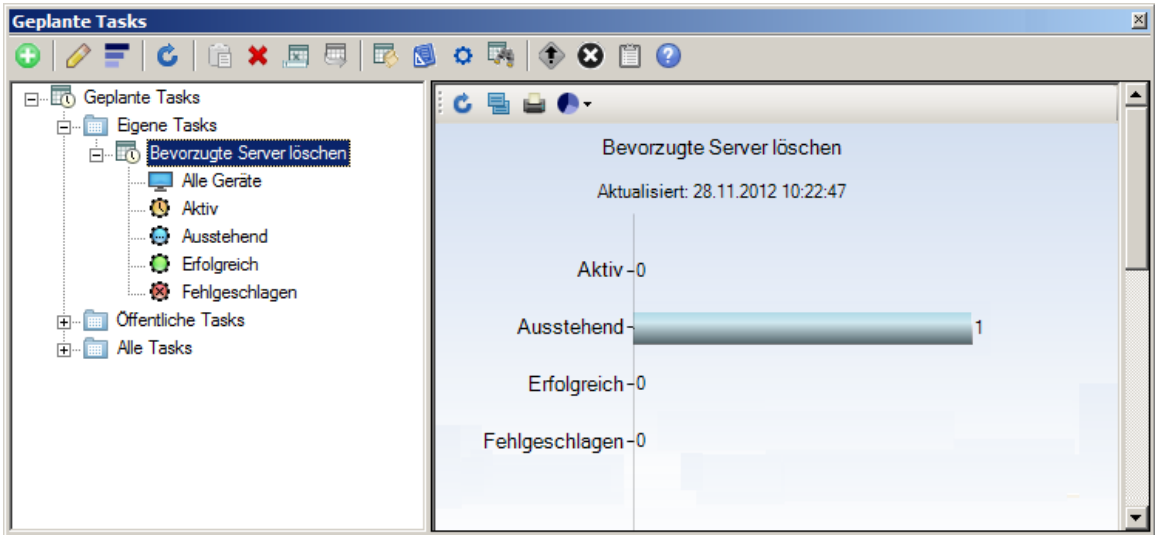
So planen Sie einen Task

1. Klicken Sie im Fenster "Geplante Tasks" auf eine der folgenden Symbolleistenschaltflächen: **Benutzerdefiniertes Skript planen, Benutzerdefinierte Datenformulare, Agentenkonfiguration** oder **Inventarscan planen**.
2. Geben Sie die für den von Ihnen ausgewählten Tasktyp erforderlichen Informationen ein.
3. Klicken Sie auf die Schaltfläche **Planen**. Hiermit wird das Fenster **Verwaltete Tasks** geöffnet, das Skript hinzugefügt und das Skript in einen Task konvertiert.
4. Wählen Sie in der Netzwerkansicht die Geräte aus, die Sie als Taskziele verwenden möchten, und ziehen Sie sie auf den Task im Fenster **Geplante Tasks**.
5. Klicken Sie im Fenster **Geplante Tasks** im Kontextmenü des Tasks auf **Eigenschaften**.
6. Legen Sie auf der Seite **Task planen** die Startzeit für den Task fest und klicken Sie auf **Speichern**.

Sie können weitere Geräte zum Task hinzufügen, indem Sie sie aus der Netzwerkansicht ziehen und im Fenster **Geplante Tasks** auf dem gewünschten Task ablegen.

Verwenden des Fensters "Geplante Tasks"

Verwenden Sie das Fenster **Geplante Tasks** zum Konfigurieren und Planen von Skripten, die Sie geschrieben haben. Planen Sie Elemente für eine einmalige Verteilung oder einen wiederkehrenden Task, z. B. einen Skript-Task für die regelmäßige Suche nach nicht verwalteten Geräten.



Das Fenster **Geplante Tasks** besteht aus zwei Hälften. In der linken Hälfte sehen Sie den Task-Baum und die eigentlichen Tasks und in der rechten Hälfte die Informationen, die sich auf die im Task-Baum ausgewählten Elemente beziehen.

Linker Fensterausschnitt

Der linke Fensterausschnitt enthält folgende Taskgruppen:

- **Eigene Tasks:** Tasks, für die Sie einen Zeitplan erstellt haben. Nur Sie selbst und administrative Benutzer von Management Suite können diese Tasks sehen.
- **Öffentliche Tasks:** Tasks, die von Benutzern mit dem Recht "Öffentlich bearbeiten" als "Öffentlich" gekennzeichnet wurden.
- **Alle Tasks:** Ihre eigenen und als globale Tasks gekennzeichnete Tasks.

Sie können Skripte in den linken Fensterausschnitt des Fensters **Geplante Tasks** ziehen. Sobald sich ein Skript im linken Fensterausschnitt befindet, können Sie Ziele für dieses Skript konfigurieren, indem Sie Geräte, Abfragen oder Gruppen in den rechten Fensterausschnitt ziehen.

Tasks weisen ferner ein Kontextmenü auf, das Sie durch Klicken mit der rechten Maustaste aufrufen können. Das Kontextmenü "Jetzt starten" bietet die folgenden Optionen:

- **Alle:** Führt den Task auf allen Zielgeräten aus.
- **Fehlgeschlagene Geräte:** Führt den Task nur auf Zielgeräten aus, die ohne Erfolg versucht haben, den Task auszuführen.
- **Geräte, die nicht versucht haben, den Task auszuführen:** Führt den Task nur auf Zielgeräten aus, die nicht versucht haben, den Task auszuführen, beispielsweise auf Zielgeräten, die nicht eingeschaltet oder nicht mit dem Netzwerk verbunden waren.
- **Im Wartezustand oder zurzeit aktiv:** Führt den Task auf Geräten aus, die sich im Wartezustand befinden oder zurzeit aktiv sind. Das ist nützlich, wenn Geräte in einen dieser Taskzustände stehengeblieben sind und Sie versuchen möchten, den Task erneut auf ihnen auszuführen.

Abbrechen eines Tasks

Sie können Tasks im Wartezustand oder aktive Tasks abbrechen. Auf welche Weise Sie den Task stornieren, hängt, wie unten beschreiben, vom Tasktyp ab.

- **Softwareverteilungstasks:** Klicken Sie in der Symbolleiste auf die Schaltfläche "Abbrechen". Diese Symbolleistenschaltfläche ist nur für Softwareverteilungstasks verfügbar.
- **Benutzerdefinierte Skripte:** Klicken Sie im Kontextmenü des Skripts, das Sie abbrechen möchten, auf **Aktuellen Status**. Das Dialogfeld **Taskstatus** verfügt über die Schaltfläche **Task aufgeben** und **Task abbrechen**. Klicken Sie auf die gewünschte Schaltfläche.
- **Tasks im Wartezustand:** Klicken Sie im Kontextmenü des Tasks, den Sie abbrechen möchten, auf **Eigenschaften**. Klicken Sie auf der Seite **Task planen** auf **Ungeplant lassen**.

Zuweisen von Zielen zu einem Task

Nachdem Sie ein Skript zum Fenster **Geplante Tasks** hinzugefügt haben, können Sie dem Task Ziele zuweisen. Ziehen Sie Ziele aus der Netzwerkansicht auf den gewünschten Task im Fenster **Geplante Tasks**. Ziele können einzelne Geräte, Gerätegruppen, LDAP-Objekte, LDAP-Abfragen und Inventarabfragen beinhalten. Abfragen und Gruppen sind leistungsstarke Optionen, mit deren Hilfe Sie eine dynamische Geräteliste erstellen können, die sich für regelmäßig wiederkehrende Tasks ändern kann. Wenn sich z. B. die aus einer Abfrage resultierenden Liste mit Zielgeräten ändert, wählen alle Tasks, die diese Abfrage verwenden, automatisch die neuen Geräte als Ziel aus.

Wenn ein Gerät mehrmals als Ziel angesprochen wird, z. B., wenn zwei Zielabfragen sich überschneidende Ergebnissen zurückgeben, erkennt der Coreserver die Überschneidung und führt den Task nicht mehrmals für dasselbe Gerät aus.

Bei Verwendung von Abfragen für Taskziele wird die Abfrage erst ausgeführt, nachdem der Task gestartet wurde. Das Dialogfeld **Geplante Tasks - Eigenschaften** zeigt die Zielgeräte erst, nachdem der Task gestartet wurde.

Anwenden von Bereichen auf Tasks

Bei geplanten Tasks können mehrere Benutzer von Management Suite Ziele zu einem Task hinzufügen. Im Fenster **Geplante Tasks** werden jedem Benutzer von Management Suite jedoch nur die Ziele innerhalb seines Bereichs angezeigt. Wenn zwei Benutzer von Management Suite mit nicht überlappenden Bereichen jeweils 20 Ziele zu einem Task hinzufügen, werden jedem Benutzer von Management Suite nur die 20 Ziele angezeigt, die er hinzugefügt hat; der Task wird jedoch auf allen 40 Zielen ausgeführt.

Auswählen von Zielen für Ihren Task

Jeder Task, den Sie erstellen, benötigt einen Satz Ziele, auf dem der Task ausgeführt wird. Tasks unterstützen zwei Zieltypen: statisch und dynamisch.

- **Statische Ziele:** Eine Liste bestimmter Geräte oder Benutzer, die ausschließlich manuell geändert werden kann. Statische Ziele können LDAP-Benutzer oder Geräte aus dem Verzeichnis-Manager oder Geräte aus der Netzwerkansicht der Konsole sein.
- **Dynamische Ziele:** Eine dynamische Liste mit Geräten, die es richtlinienbasierten Verteilungstasks gestattet, die Zielliste in regelmäßigen Abständen auf Änderungen zu überprüfen. Zu dynamischen Zielen gehören Abfrageergebnisse, LDAP-Gruppen/-Container und Gruppen in der Netzwerkansicht.

Dynamische Richtlinienziele sind insofern einmalig, als Management Suite die Ergebnisse dieser Abfragen periodisch aktualisiert. Wenn neue Geräte die Abfragekriterien erfüllen, werden wiederkehrende Tasks, die diese Abfragen verwenden, auf die neuen Geräte angewendet.

Es gibt folgende Möglichkeiten, statische Richtlinienziele anzugeben:

- **Netzwerkansicht-Geräte:** Eine statische Gruppe von Geräten aus der Coredatenbank.
- **LDAP-Benutzer oder -Geräte:** Eine statische Gruppe von Benutzer- und/oder Geräteobjekten.

Es gibt folgende Möglichkeiten, dynamische Richtlinienziele anzugeben:

- **Netzwerkansicht-Gruppe:** Eine dynamische Gruppe von Geräten aus der Coredatenbank.
- **LDAP-Gruppe/-Container:** Ein dynamischer Satz aus Benutzer-, Geräte- oder Gruppenobjekten.
- **Datenbankabfrage:** Eine Gruppe von Geräten, die mithilfe einer Abfrage der Coredatenbank generiert wird..
- **Benutzergruppe:** Eine Gruppe von Benutzern, die aus einem LDAP-kompatiblen Verzeichnis ausgewählt wird.
- **LDAP-Abfrage:** Eine Gruppe von Benutzern, Geräten oder beidem, die mithilfe einer Abfrage eines LDAP-kompatiblen Verzeichnisses generiert wird.

Auswählen von Zielgeräten über ein Verzeichnis

Damit Geräte Richtlinien empfangen können, die über Active Directory als Ziele angesprochen werden, müssen die Geräte für die Anmeldung beim Verzeichnis konfiguriert sein. Das bedeutet, dass die richtige Geräte-Software installiert sein muss. Außerdem müssen sich die Geräte beim richtigen Verzeichnis anmelden, damit ihr eindeutiger, definierter Name dem Namen entspricht, der über den Verzeichnis-Manager angegeben wurde.

Für jedes Windows-Gerät muss es ein Computerkonto auf dem Active Directory-Domänencontroller geben. Das heißt, der als Gerät verwendete Computer muss bei der Domäne angemeldet sein, in der Active Directory gespeichert ist. Sie können nicht einfach ein Netzlaufwerk mit dem voll qualifizierten Windows-Domänennamen verbinden. Die Richtlinie wird in diesem Fall nicht angewendet.

So verwenden Sie den Verzeichnis-Manager zum Erstellen einer Abfrage

1. Klicken Sie auf **Extras > Verteilung > Verzeichnis-Manager**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Verzeichnis verwalten**.
3. Geben Sie den Verzeichnis-URL und die Authentifizierungsdaten ein und klicken Sie auf **OK**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Abfrage**.
5. Erstellen Sie die Abfrage. Weitere Informationen finden Sie unter "LDAP-Abfragen" auf Seite 195.

Was Sie bei der Ausführung von Tasks sehen

Im Fenster **Geplante Tasks** wird immer der Auftragsstatus angezeigt. Wenn Sie Gerätekonfigurationen oder Betriebssystembereitstellungen planen, wird zudem das Dialogfeld **Client Setup-Dienstprogramm** angezeigt. Während der Schedulerdienst die Zielliste abarbeitet, werden Listen mit den zu konfigurierenden Geräten, Geräten, die gerade konfiguriert werden, und vollständig konfigurierten Geräte angezeigt. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "Agentenkonfigurationstool"" auf Seite 145.

Wenn Sie die Verteilung über Targeted Multicast planen, wird der Status im Fenster **Multicast Software Distribution-Status** angezeigt. Dieses Fenster zeigt den Multicast-Status an. Weitere Informationen finden Sie unter "Das Statusfenster "Multicast Software Distribution"" auf Seite 312

Wenn Sie benutzerdefinierte Skripte planen, wird das Fenster **Benutzerdefinierte Jobverarbeitung** eingeblendet, das die geplanten, laufenden und abgeschlossenen Zielgeräte sowie den Skriptstatus Zeile für Zeile anzeigt, während das Skript ausgeführt wird.

Überwachen des Taskstatus

Sobald die Taskverarbeitung beginnt, durchlaufen Zielgeräte mehrere Taskzustände. Sie können den Taskstatus für Zielgeräte überwachen, indem Sie auf einen aktiven Task im Fenster **Geplante Tasks** klicken. Die Geräte befinden sich in einer der folgenden Kategorien:

- **Alle Geräte:** Alle Ziele für den Task.
- **Aktiv:** Ziele, die zurzeit verarbeitet werden.
- **Ausstehend:** Ziele, die noch nicht verarbeitet wurden.
- **Erfolgreich:** Ziele, die den Task erfolgreich ausgeführt haben.
- **Fehlgeschlagen:** Ziele, auf denen der Task misslungen ist.

Dies sind die Zustände, die für das Gerät gelten können, und die Kategorien, in denen sie sichtbar sind:

- **Wartezustand:** Zur Verarbeitung eines Tasks bereit; Kategorie (**Ausstehend**)
- **Aktiv:** Verarbeitung des aktuellen Tasks; Kategorie (**Aktiv**).
- **Fertig:** Task wurde erfolgreich ausgeführt; Kategorie (**Erfolgreich**).
- **Beschäftigt:** Gerät verarbeitet bereits einen anderen Task und kann den aktuellen Task nicht übernehmen; Kategorie (**Fehlgeschlagen**).
- **Fehlgeschlagen:** Die Verarbeitung des Tasks wurde aus irgendeinem Grund abgebrochen; Kategorie (**Fehlgeschlagen**).
- **Aus:** Gerät war ausgeschaltet oder nicht erreichbar; Kategorie (**Fehlgeschlagen**).
- **Abgebrochen:** Der Benutzer hat den Task abgebrochen; Kategorie (**Fehlgeschlagen**)

Anzeigen von Taskprotokollen

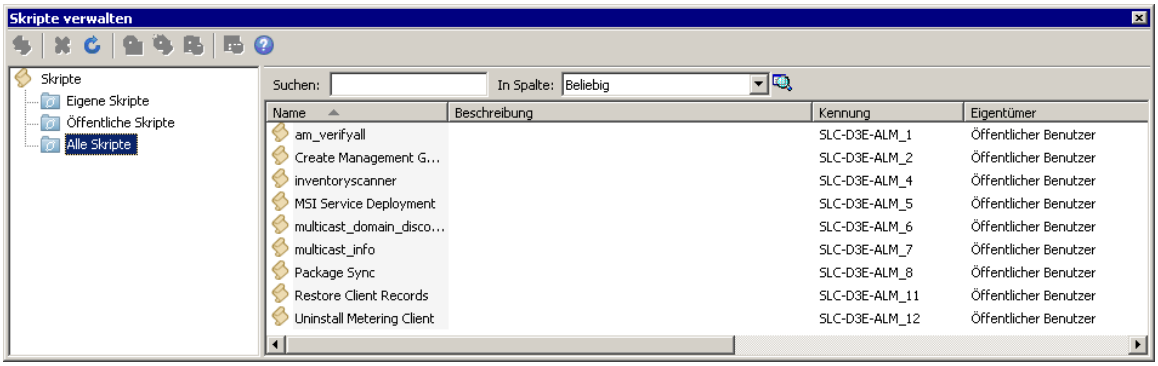
Wenn es einem Gerät nicht gelingt, einen Task zu verarbeiten, wird im Fenster **Geplante Tasks** ein Taskprotokoll gespeichert. Verfügbare Protokoll werden in der Spalte **Protokolldatei** neben einem Gerät angezeigt. In der Protokolldatei können Sie den Taskbefehl, dessen Ausführung misslungen war, anzeigen.

Verwenden der Standardskripte

Management Suite wird meinen Standardsatz von Skripten geliefert, die im Folgenden aufgeführt sind. Diese Skripte können Sie bei der Ausführung häufig anfallender Management Suite-Tasks unterstützen. Die Skripte befinden sich in der Strukturansicht **Alle anderen Skripte** im Fenster **Skripte verwalten** (**Extras > Verteilung > Skripte verwalten**).

- **am_verifyall:** Alle Pakete, die über Richtlinien auf Clients installiert wurden, werden überprüft.
- **Management Gateway-Clientzertifikat erstellen:** Erstellt ein Sicherheitszertifikat, damit ein Gerät einen Management Gateway verwenden kann.
- **inventoryscanner:** Führt den Inventarscanner auf den ausgewählten Geräten aus.

- **multicast_domain_discovery:** Es wird eine Multicast-Domänenrepräsentantenerkennung ausgeführt.
- **multicast_info:** Es wird ein Problembehandlungsskript ausgeführt, das anzeigt, welche Informationen das Fenster "Geplante Tasks" an Targeted Multicast weitergibt, einschließlich der IP-Adressen des Zielgeräts sowie Subnetzinformationen. Erstellt eine Datei mit dem Namen c:\mcinfo.txt.
- **Paketsynchronisierung:** Führt eine Richtlinienprüfung durch, um festzustellen, ob neue Richtlinien angewendet oder zur Verfügung gestellt werden müssen.
- **Clientdatensätze wiederherstellen:** Führt den Inventarscanner auf ausgewählten Geräten aus, der Scanner berichtet jedoch an den Core, auf dem das Gerät konfiguriert wurde. Wenn Sie die Datenbank zurücksetzen müssen, hilft Ihnen dieser Task, die Geräte in einer Umgebung mit mehreren Cores wieder der richtigen Datenbank zuzuordnen.
- **Überwachungsclient deinstallieren:** Entfernt den Softwareüberwachungsagent auf Zielgeräten. Dieser Agent wurde in Management Suite vor Version 8 eingesetzt.



Grundlegendes zu den Bandbreitenoptionen für Tasks

Beim Konfigurieren von Local Scheduler-Befehlen können Sie angeben, welche Bandbreitenkriterien mindestens erfüllt sein müssen, damit der Task ausgeführt werden kann. Der Bandbreitentest besteht aus Netzwerkdaten, die an ein von Ihnen angegebenes Gerät übermittelt werden. Zu dem Zeitpunkt, zu dem der Task ausgeführt werden soll, sendet jedes Gerät, das den Local Scheduler-Task ausführt, eine kleine Menge ICMP-Netzwerkdaten an den von Ihnen angegebenen Gerät und wertet die Übertragungsleistung aus. Wenn das Zielgerät für den Test nicht verfügbar ist, wird der Task nicht ausgeführt.

Sie können folgende Bandbreitenoptionen auswählen:

- **RAS:** Der Task wird ausgeführt, wenn die Netzwerkverbindung des Geräts mit dem Zielgerät mindestens RAS- oder DFÜ-Geschwindigkeit erreicht (wie vom Netzwerk-API erkannt). Wenn Sie diese Option auswählen, bedeutet dies im Allgemeinen, dass der Task immer ausgeführt wird, wenn das Gerät über eine Netzwerkverbindung verfügt.
- **WAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielgerät mindestens WAN-Geschwindigkeit erreicht. WAN-Geschwindigkeit wird als Nicht-RAS-Verbindung definiert, die langsamer als der LAN-Grenzwert ist.
- **LAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielgerät die LAN-Geschwindigkeitseinstellung überschreitet. Als LAN-Geschwindigkeit wird standardmäßig jede Geschwindigkeit von mehr als 262.144 Bit/s definiert. Sie können den LAN-Grenzwert in der Agentenkonfiguration festlegen (Seite **Extras > Konfiguration > Agentenkonfiguration, Bandbreitenerkennung**). Die Änderungen werden erst wirksam, nachdem Sie die aktualisierte Konfiguration auf Geräten bereitgestellt haben.

Verwenden des Rollup-Cores zum Planen globaler Tasks

Wenn in Ihrer LANDesk-Umgebung ein Rollup-Core installiert ist, können die auf diesem Rollup-Core erstellten Tasks global geplant werden; darüber hinaus unterstützen diese Tasks Ziele von unterschiedlichen Child-Cores. Wenn Sie einen Task auf dem Rollup-Core erstellen und planen, überprüft der Rollup-Core in der Zielliste, welche Ziele zu welchem Child-Coreserver gehören. Der Rollup-Core sendet dann den Task und den zugehörigen eindeutigen Abschnitt der Gesamt-Zielliste an die einzelnen Child-Coreserver. Jeder Child-Coreserver führt den Task im Hintergrund aus und gibt den Taskstatus an den Rollup-Core zurück.

Wenn ein Child-Core zwar Ziele hat, aber über keine Rollup-Core-Zertifikate verfügt (eine Voraussetzung, damit ein Child-Core global geplante Tasks verarbeiten kann), führt der Rollup-Core den Task stattdessen auf diesen Zielen aus.

Global geplante Tasks und der Taskstatus werden nicht im Fenster **Geplante Tasks** des Child-Cores angezeigt. Die einfachste Möglichkeit, diese Informationen anzuzeigen, ist über die Taskdetails auf dem Rollup-Core. Wenn Sie den Status des delegierten Tasks auf einem Child-Core anzeigen möchten, der den Task verarbeitet, können Sie den Bericht "Delegierte Tasks" verwenden.

HINWEIS: Von einem Rollup-Core der Version 9.0 und höher geplante Tasks, einschließlich sicherheitsbezogener Tasks, funktionieren auf Cores der Versionen 8.7 und 8.8 nicht.

So zeigen Sie den Status eines delegierten Tasks auf einem Child-Core an

1. Klicken Sie auf dem Child-Core auf **Extras > Berichte/Überwachung > Berichte**.
2. Klicken Sie im Fenster "Berichte" auf **Berichte > Management Suite > Taskstatus**.
3. Doppelklicken Sie auf den Bericht **Delegierte Tasks** und geben Sie den gewünschten Datumsbereich ein.
4. Klicken Sie auf **OK**, um den Bericht anzuzeigen.

Um das Datenaufkommen im Netzwerk zu reduzieren, wird der Taskstatus für delegierte Tasks nicht in Echtzeit auf dem Rollup-Core registriert. Stattdessen wird der Taskstatus standardmäßig alle 2 Minuten aktualisiert. Führen Sie die nachfolgenden Schritte aus, um dieses Intervall zu ändern.

So ändern Sie das Intervall zur Überprüfung des Taskstatus

1. Klicken Sie auf dem Rollup-Core auf **Start > Programme > LANDesk > LANDesk Dienste konfigurieren**.
2. Klicken Sie auf der Registerkarte **Scheduler** auf **Erweitert**.
3. Klicken Sie auf **Statusprüfung für delegierten Task** und klicken Sie auf **Bearbeiten**.
4. Geben Sie an, wie viele Sekunden der Scheduler zwischen den Taskstatusprüfungen warten soll, und klicken Sie auf **OK**. Der Standardwert ist 120 Sekunden.
5. Klicken Sie auf der Registerkarte **Scheduler** auf **Neu starten**, um den Scheduler-Dienst auf dem Rollup-Core neu zu starten.

Local Scheduler

Informationen zum Local Scheduler

Der Local Scheduler ist ein Dienst, der auf Geräten ausgeführt wird. Er ist Teil des Common Base Agent und kann über das Gerätesetup installiert werden. Im Allgemeinen verwaltet der Local Scheduler Management Suite Aufgaben, beispielsweise die regelmäßige Ausführung des Inventarscanners. Andere zeitplangesteuerte Tasks, z. B. Software- oder Betriebssystembereitstellungen, werden nicht vom Local Scheduler sondern vom Coreserver ausgeführt. Sie können mit dem Local Scheduler eigene Tasks für die regelmäßige Ausführung auf Geräten planen. Sobald Sie ein Local Scheduler-Skript erstellt haben, können Sie es mithilfe des Fensters **Geplante Tasks** auf relevanten Geräten bereitstellen.

Der Local Scheduler weist jedem Task eine Kennnummer zu. Der Kennungsbereich der Local Scheduler-Skripte unterscheidet sich von den Standardskripten des Local Schedulers, mit denen Management Suite arbeitet. Standardmäßig darf auf jedem Gerät immer nur ein benutzerdefiniertes Scheduler-Skript aktiv sein. Wenn Sie ein neues Skript erstellen und auf Geräten bereitstellen, ersetzt das neue Skript das alte Skript (jedes Skript im benutzerdefinierten Kennungsbereich des Local Schedulers), ohne sich auf die Standardskripte des Local Schedulers (beispielsweise den Zeitplan für den lokalen Inventarscan) auszuwirken.

Installation des Local Scheduler-Dienstes auf einem nicht verwalteten Gerät

Der LANDesk Local Scheduler-Dienst kann auf einem nicht verwalteten Gerät installiert werden. Sie benötigen nur zwei Dateien für die Funktionalität des Local Schedulers:

- LocalSch.exe
- LTapi.dll

Um den LANDesk Local Scheduler-Dienst auf einem/einer nicht verwalteten Server oder Arbeitsstation zu installieren, gehen Sie folgendermaßen vor:

1. Erstellen Sie folgenden Ordner.

```
%ProgramFiles%\LANDesk\LDClient
```

2. Kopieren Sie LocalSch.exe und LTapi.dll in diesen Ordner.
3. Klicken Sie auf **Start > Ausführen** und geben Sie den folgenden Befehl ein.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /i
```

Deinstallation des Local Scheduler-Dienstes

Um den LANDesk Local Scheduler-Dienst zu deinstallieren, gehen Sie folgendermaßen vor:

1. Klicken Sie auf Start > Ausführen und geben Sie den folgenden Befehl ein.

```
"%ProgramFiles%\LANDesk\LDClient\localsch.exe" /r
```

2. Löschen Sie die Dateien und Ordner.

Mit LocalSch.exe einen Task hinzufügen

Die restlichen Befehlzeilenparameter werden zum Hinzufügen eines lokalen Tasks verwendet. Beim Hinzufügen eines Tasks müssen Sie die Anwendungsdatei mit dem /exe-Parameter angeben. Wenn der Benutzer oder der Prozess, der die Befehlszeile ausführt, keine administrativen Rechte hat, wird der Task nicht geplant. Wenn der aktuelle Benutzer nicht über administrative Privilegien verfügt, wird der Task nicht erstellt.

Zusätzlich zu den unten beschriebenen Befehlszeilenoptionen kann auch die /taskid-Option zum Angeben des Tasks verwendet werden.

/exe=<executable> - Geplante Anwendung

Gibt die Anwendung an, die zur geplanten Zeit gestartet werden soll. Ohne diesen Parameter wird der lokale Task nicht erstellt.

/cmd=<command line> - Anwendungsbefehlszeile

Gibt die Befehlszeile an, die verwendet werden soll, wenn die geplante Anwendung gestartet wird. Ohne Angabe dieses Parameters wird die geplante Anwendung ohne die Befehlszeilenparameter gestartet.

/start="<date/time>" – Startzeit

Gibt die Startzeit der Anwendung an. Ohne Angabe dieses Parameters wird die Anwendung zum nächstmöglichen Zeitpunkt gestartet. Falls etwaige Filter angegeben sind, müssen diese vor dem Start der Anwendung durchgeführt werden. Die Startzeit wird in der örtlichen Systemzeit des Computers im folgenden Format angegeben:

```
/start="06 Nov 2001 17:39:47" /bw=WAN|myserver.domain.com
```

Dies ist eine abgekürzte Version des HTTP-Formats. Der Monat wird immer als dreistellige ASCII-Abkürzung angegeben: Jan, Feb, Mär, Apr, Mai, Jun, Jul, Aug, Sep, Okt, Nov oder Dez. Wird das Datum im falschen Format angegeben, dann wird der Task nicht hinzugefügt.

/freq=xxx – Häufigkeit

Gibt eine zyklische Häufigkeit an. Die Häufigkeit gibt an, nach wie vielen Sekunden der Task erneut ausgeführt wird. Ist dieser Parameter nicht angegeben oder Null, wird der Task nur einmal ausgeführt.

/user – Benutzerfilter

Gibt an, dass ein Filter für den Task erstellt werden sollte. Ein Benutzerfilter verhindert, dass der Task ausgeführt wird, bevor ein Benutzer am System angemeldet ist.

/bw=xxx|<network host> - Bandbreitenfilter

Gibt an, wie viel Bandbreite für einen bestimmten Netzwerkhost benötigt wird. Die Bandbreite kann als LAN, WAN oder RAS angegeben werden. Wird ein anderer Bandbreitenwert verwendet, dann stellt der Local Scheduler die Bandbreite automatisch auf RAS ein. Der Task wird nicht ausgeführt, bis der Local Scheduler erkennt, dass die angegebene Bandbreite zwischen dem Gerät und dem angegebenen Netzwerkhost zur Verfügung steht.

Der folgende Filter gibt z. B. an, dass der Task nicht ausgeführt wird, bevor mindestens WAN-Konnektivität zum myserver.domain.com-Rechner zur Verfügung steht.

```
/bw=WAN|myserver.domain.com
```

/tod=<begin>|<end> - Tageszeitfilter

Gibt einen Tageszeitfilter an. Der Task wird nur zu der zwischen der Anfangs- und Endstunde liegenden Tageszeit ausgeführt. Tageszeitwerte werden in Stunden unter Verwendung der Werte 0 bis 23 angegeben. Der folgende Filter würde z. B. einen Task zwischen 19:00 und 22:00 Uhr ausführen.

```
/tod=19|22
```

/dow=<begin>|<end> - Wochentagfilter

Gibt einen Wochentagfilter an. Der Task wird nur zu der zwischen den angegebenen Anfangs- und Endtagen ausgeführt. Wochentagswerte werden als Ganzzahl angegeben, wobei 0 Sonntag ist. Der folgende Filter würde beispielsweise angeben, dass ein Task zwischen Sonntag und Donnerstag ausgeführt werden soll.

```
/dow=0|4
```

/dom=<begin>|<end> - Datumsfilter

Gibt einen Datumsfilter an. Der Task wird nur an Tagen zwischen dem angegebenen Anfangs- und Enddatum ausgeführt. Der Datumsfilter wird als numerischer Wert zwischen 1 und 31 angegeben. Der folgende Filter würde beispielsweise angeben, dass der Task zwischen dem 16. und dem 28. des Monats ausgeführt werden soll.

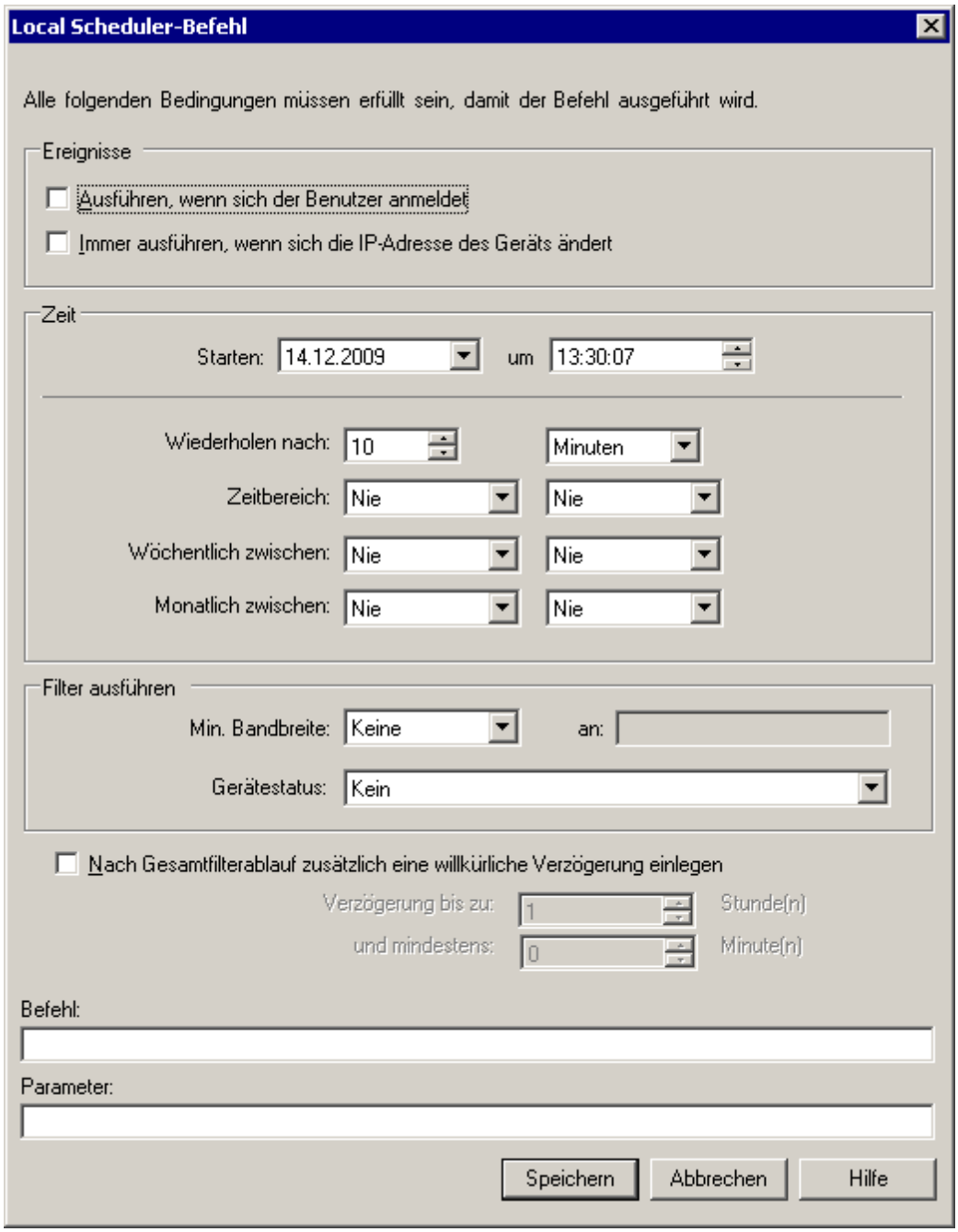
```
/dom=16|28
```

/ipaddr - IP-Adressenänderungsfilter

Gibt an, dass der Task immer ausgeführt werden muss, wenn sich die IP-Adresse des Geräts ändert.

Erstellen eines Local Scheduler-Befehls

Gehen Sie bei der Auswahl der Zeitplanoptionen nicht so restriktiv vor, dass die Kriterien für den Task selten erfüllt werden, es sei denn, dass ist Ihre Absicht. Beispiel: Wenn Sie beim Konfigurieren eines Task als Wochentag den Montag auswählen und den 17. als Tag des Monats, wird der Task nur an einem Montag ausgeführt, der auch gleichzeitig der 17. des Monats ist; dieser Fall tritt jedoch nur sehr selten ein.



So erstellen Sie einen Befehl im Local Scheduler

1. Klicken Sie im Fenster **Verwaltete Skripte** (**Extras > Verteilung > Skripte verwalten**) im Kontextmenü "Eigene Skripte" auf **Neues Local Scheduler-Skript**.
2. Geben Sie einen **Skriptnamen** ein.
3. Klicken Sie auf **Hinzufügen**, um die Optionen für das Skript zu definieren.
4. Konfigurieren Sie die Local Scheduler-Optionen wie bereits beschrieben.
5. Klicken Sie auf **Speichern**, um Ihr Skript zu speichern.

6. Verwenden Sie das Fenster **Geplante Tasks**, um das Skript, das Sie erstellt haben, auf Geräten bereitzustellen.

Löschen eines Tasks mit LocalSch.exe

Der Local Scheduler kann einen oder mehrere Tasks löschen. Beim Löschen eines Tasks werden die folgenden Parameter verwendet.

/del – Task oder Tasks löschen

Löscht den durch den /taskid-Parameter angegebenen Task oder alle Tasks im Bereich "/range", einschließlich dem Höchst- und Mindestwert. Die Taskkennungen können entweder festgelegt werden, indem Sie sie mit der /task-Befehlszeilenoption anzeigen oder eine konstante /taskid beim Hinzufügen eines Tasks verwenden.

/removetasks – Alle Tasks entfernen

Entfernt alle zurzeit geplanten lokalen Tasks.

/taskid – Angabe der Taskkennung

Gibt die Kennung des zu löschenden Tasks an. Taskkennungen können festgestellt werden, indem Sie die zurzeit geplanten Tasks ansehen (s.o. /tasks). Die Kennung wird als Ganzzahl angegeben.

/range=<min>|<max> – Bereich der Taskkennungen

Gibt einen Mindest- und Höchstwert eines Taskkennungsbereichs an. Sie können ihn mit dem /entf-Befehl verwenden, um alle Tasks mit Taskkennungen im angegebenen Bereich zu löschen.

Normalerweise wird die Taskkennung beim Erstellen eines Tasks willkürlich mit dem aktuellen Zeitwert (time_t) zugewiesen. Eine willkürlich zugewiesene Kennung liegt niemals unter 100000. Dieser Befehlszeilenparameter kann verwendet werden, um die Kennung für den Task anzugeben. Die Taskkennungswerte 0 bis 1000 sind für die interne Verwendung der LANDesk Software reserviert. Die Taskkennungswerte 1001-2000 sind für die Verwendung der lokalen Scheduler-Schnittstelle der Managementkonsole vorbehalten.

LocalSch.exe Befehlszeilenparameter

Zusätzlich zur Überwachung und Ausführung lokaler Tasks können Sie LocalSch.exe noch zum Installieren und Entfernen des Dienstes, zum Hinzufügen neuer Tasks und Ausführen aller derzeit konfigurierten Tasks verwenden.

Im Folgenden sehen Sie die Befehlszeilenoptionen, die von der Local Scheduler-Anwendung unterstützt werden.

```
LocalSch.exe [/i] [/r] [/d] [/tasks] [/isinstalled] [/del] [/removetasks]
 [/exe=<executable>] [/cmd=<command line>] [/start=”<date/time>”] [/freq=xxx]
 [/user] [/bw=xxx|<server>] [/tod=<begin>|<end>] [/dow=<begin>|<end>]
 [/dom=<begin>|<end>] [/ipaddr] [/taskid=<id>] [/range=<min>|<max>]
```

/i – Installationsdienst

Installiert den Local Scheduler-Dienst auf dem Gerät. Nach der Installation muss der Local Scheduler dennoch gestartet werden.

/r – Dienst entfernen

Entfernt den Local Scheduler-Dienst vom Gerät. Der Local Scheduler-Dienst sollte vor dem Entfernen beendet werden.

/d – In Fehlersuchmodus ausführen

Führt den Local Scheduler in einem Fehlersuchmodus aus. Wenn der Local Scheduler in Fehlersuchmodus ausgeführt wird, läuft er als normaler Windows-Prozess - nicht als ein Dienst oder Pseudodienst. Dieser Modus führt nicht zu zusätzlichen Fehlersuchausgaben.

/isinstalled – Installationsprüfung

Prüft, ob der Local Scheduler-Dienst auf dem lokalen Rechner installiert ist. Diese Methode gibt S_OK oder Null aus, wenn der Local Scheduler installiert ist. Ist Local Scheduler nicht installiert, wird ein anderer Wert als Null ausgegeben.

/tasks – Tasks ausführen

Dieser Befehl leitet die aktuell konfigurierten Tasks an stdout weiter, kann aber nur dann in der Befehlszeile angezeigt werden, wenn der Befehl mit mehreren weiteren zusammenhängt.

```
LocalSch.exe /tasks | mehr
```

Die Ausgabe kann mit der folgenden Befehlszeile in eine Textdatei umgeleitet werden (z. B. tasks.txt):

```
LocalSch.exe /tasks > tasks.txt
```

Local Scheduler-Zeichensatzanalyse und die Befehlszeile

Der Local Scheduler verwendet standardmäßig durch Leerstellen begrenzte Zeichensatzanalyse für die Befehlszeile. D.h. wenn einer der Parameter eine Leerstelle enthält, muss er durch Anführungszeichen eingeschlossen werden. Gewisse Parameter, wie z. B. /start, enthalten immer Leerstellen und müssen daher immer in Anführungszeichen stehen. Andere Parameter, z. B. /exe und /cmd, können Leerstellen enthalten oder auch nicht, und müssen daher nicht unbedingt in Anführungszeichen stehen.

Das folgende Beispiel zeigt eine Befehlszeile, die keine Anführungszeichen benötigt.

```
LocalSch.exe /exe=c:\windows\system32\cmd.exe
```

Das folgende Beispiel zeigt eine Befehlszeile, die Anführungszeichen benötigt.

```
LocalSch.exe /exe="%ProgramFiles%\MyProgram\myprog.exe" /cmd="/apm /s /ro"
```

Anführungszeichen um Parameter, die bereits in Anführungszeichen stehen

Wenn die an /cmd zu übergebenen Parameter bereits in Anführungszeichen stehen, dann sind drei Anführungszeichen nötig: Ein Satz für die gesamte Zeichenfolge. Ein weiterer, um die Werte in Anführungszeichen in Anführungszeichen zu setzen und die der Werte in Anführungszeichen.

Die folgende Befehlszeile zeigt ein Beispiel für Parameter, die von drei Anführungszeichen umgeben sein müssen.

```
LocalSch.exe /exe="%ProgramFiles%\LANDesk\File Replicator\LANDeskFileReplicatorNoUI.exe"
/cmd="""%ProgramFiles%\LANDesk\File Replicator\LDHTTPCopyTaskConfig.xml"" ""%ProgramFiles%\LANDesk\File
Replicator\replicator.log"""
```

Im o.g. Befehl stellen die beiden Parameter Dateipfade dar. Weil sich beide Pfade im Verzeichnis "Programme" befinden, haben ihre Pfade Leerstellen und müssen in Anführungszeichen gesetzt werden, um korrekte Parameter für LANDeskFileReplicatorNoUI.exe darzustellen. Daher ist jeder Parameter in Anführungszeichen von einem zweiten Satz Anführungszeichen und die gesamte Zeichenfolge von weiteren Anführungszeichen umschlossen.

Redirection-Operator in Anführungszeichen setzen

Auch Switches, die einen Redirection-Operator enthalten, müssen in Anführungszeichen gesetzt werden. Redirection-Operator haben folgende Symbole: <, >, |. Der /bw-Switch verwendet ein |-Zeichen, das wir Strich oder Balken nennen. Es ist wichtig, daran zu denken, dass das |-Zeichen in der Befehlsaufforderung die Ausgabe an eine andere Anwendung trennt. Um zu vermeiden, dass dieses Zeichen von der Befehlszeile analysiert wird, muss es in Anführungszeichen gesetzt werden.

Der folgende Befehl verwendet beispielsweise einen /bw-Parameter mit einem |-Zeichen und muss in Anführungszeichen stehen.

```
LocalSch.exe /exe=C:\ldclient\myprogram.exe /cmd="/apm /s /ro" /bw="LAN|server"
```

Remotesteuerung

Verwenden des Remote Control Viewers

Den "Remote Control Viewer" verwenden Sie, um aus der Ferne auf ein Gerät zuzugreifen. Die Remotesteuerung wird nur von Geräten unterstützt, auf denen der Remotesteuerungsagent installiert ist. Während einer Remotesteuerungssitzung verfügt das Remotegerät über zwei Benutzer – Sie und den Benutzer, der am Remotegerät sitzt. Sie können am Remotegerät alle Aktionen durchführen, die auch der Benutzer durchführen kann, der an diesem Gerät sitzt.

Wenn der Geräteagent entsprechend konfiguriert wurde (in der Agentenkonfiguration des Geräts), können Sie den Benutzer auch auffordern, vor der Initiierung einer jeden neuen Sitzung seine Genehmigung zu erteilen.

Sobald die Verbindung hergestellt ist, wird in der linken oberen Ecke des Fensters vom Benutzer das Remote-Statussymbol angezeigt.

Hierdurch wird der Benutzer darauf aufmerksam gemacht, dass sein Gerät remote gesteuert wird. Der Benutzer kann jederzeit durch Rechtsklick auf das Symbol sehen, ob die Sitzung noch aktiv ist, wer die Remotesteuerung hat usw.

Vom Viewer-Fenster aus sind mehr Funktionen verfügbar als nur die reine Remotesteuerung. Sobald der Viewer die Verbindung zu einem Gerät herstellt, stehen die folgenden Tasks in der Symbolleiste zur Auswahl.

- **Verbinden/Verbindung trennen** Starten bzw. Beenden einer Remotesteuerungssitzung.
- **Remotecomputeransicht starten/anhalten:** Anzeigen bzw. Ausblenden des Bildschirms des Remotegeräts im Remote Control Viewer.
- **Chat:** So chatten Sie mit einem Benutzer an einem Remotegerät
- **Dateiübertragung:** Für die Übertragung von Dateien auf und von Ihrem Computer auf ein Remotegerät. Dies funktioniert im Wesentlichen so als ob Sie ein Laufwerk einem Remotegerät zugeordnet haben.
- **Neu starten:** Für Remoteneustarts eines Geräts.
- **Zeichnen:** Zeigt Zeichentools an, mit dem Sie auf dem Remotebildschirm zeichnen können.

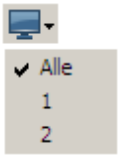
Sie können mehrere Viewer-Tasks gleichzeitig auf einem Gerät ausführen. Wenn Sie einen Viewer-Task aktivieren, wird die Benutzeroberfläche für den jeweiligen Task im Viewer-Fenster eingeblendet.

Über die Symbolleiste können Sie auch steuern, wie das Remotegerät auf Ihrem Bildschirm angezeigt wird. Zum Beispiel:

- **Im Vollbildmodus anzeigen:** Diese Option verwenden Sie, um den Remotebildschirm auf Ihrem lokalen Bildschirm im Vollbildmodus anzuzeigen. Wenn die Auflösung des Remotebildschirms höher ist als die Ihres Bildschirms, müssen Sie unter Umständen die Funktion für den automatischen Bildlauf (siehe unten) verwenden, es sei denn, Sie haben die Option **An Bildschirmgröße anpassen** aktiviert.

- **An Bildschirmgröße anpassen:** Da das Viewer-Fenster unter Umständen nicht so groß ist, wie der Bildschirm des Remotegeräts, können Sie diese Option verwenden, um den Bildschirm des Benutzers an die Größe des sichtbaren Bereichs auf Ihrem Bildschirm anzupassen.

- **Multimonitor:** Wenn der Benutzer über mehr als einen Bildschirm verfügt, wird diese Schaltfläche automatisch aktiviert, und Sie können dann in Ihrem Remote-Fenster zwischen (bis zu 8) Bildschirmen hin- und herschalten. Sie können jeden der Remote-Bildschirme minimieren oder dessen Größe ändern, um sich die Arbeit innerhalb Ihres Remotesteuerungsfenster zu erleichtern.

  Wenn Sie die Option **Alle** auswählen, wird die Größe aller Bildschirme automatisch so angepasst, dass sie alle in das Remote Control Viewer-Fenster passen. Anschließend können Sie jeden beliebigen Bildschirm auswählen und dessen Größe durch Ziehen ändern, um sich so die Arbeit mit den Bildschirmen zu vereinfachen.

Die Symbolleiste enthält ferner eine Schaltfläche „Ausführen“, mit der Sie ein ausführbares Programm auf dem Remotegerät ansteuern und ausführen können.

Die Funktion **Automatischen Bildlauf zulassen** (**Extras > Optionen > Einstellungen ändern > Automatischen Bildlauf zulassen**) verwenden Sie, um einen Bildlauf nach oben, nach unten oder von einer Seite zur anderen durchzuführen. Bei AutoBildlauf erfolgt der Bildlauf im Fenster automatisch, wenn der Mauszeiger zum Fensterrand bewegt wird.

Der Anzeigebereich des Viewer-Fensters kann durch Deaktivieren von Objekten im Ansichtsmenü (wie z. B. Verbindungsmeldungen, Symbolleiste oder Statusleiste) erweitert werden.

Wenn Sie die Ansichtsrate erhöhen oder die Einstellungen des Viewer-Fensters ändern möchten, verwenden Sie die Optionen der Schaltfläche **Optimieren** in der Symbolleiste.

Verbindungsherstellung zu Remotegeräten

Bevor Sie Tasks über Remotesteuerung ausführen können, müssen Sie eine Verbindung zum Zielgerät herstellen. Sie können die Verbindung direkt oder über ein LANDesk Management Gateway herstellen. Es kann nur ein Viewer gleichzeitig mit dem Gerät kommunizieren. Sie können jedoch mehrere Viewer-Fenster öffnen und verschiedene Geräte gleichzeitig steuern. Wenn Sie eine Verbindung zu einem Gerät herstellen, sehen Sie die Verbindungsmeldungen und den Status im Bereich **Verbindungsmeldungen**, wenn dieser sichtbar ist. Andernfalls können Sie durch Klicken auf **Ansicht > Verbindungsmeldungen** umschalten.

So stellen Sie eine Verbindung zu einem Gerät her

1. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf das Gerät, das Sie per Remotesteuerung bedienen möchten, und klicken Sie dann auf **Remotesteuerung**, Chat, **Dateiübertragung** oder **Remoteausführung**.
2. Sobald das Viewer-Fenster angezeigt wird und die Verbindung mit dem Remotegerät hergestellt wurde, können Sie jedes beliebige Remotesteuerungstool verwenden, das im Menü **Extras** des Viewers zur Verfügung gestellt wird, beispielsweise Chat, Dateiübertragung, Neustart, Inventar oder

Remotesteuerung.

3. Zum Beenden einer Remotesteuerungssitzung klicken Sie auf **Datei > Verbindung beenden**.

Verwenden der Zeichentools auf Remotegeräten

Wenn Sie ein Gerät remote anzeigen, können Sie die Zeichentools des Geräts verwenden. Mithilfe der Zeichentools können Sie Benutzern erklären, was Sie gerade tun, oder Sie können Daten auf dem Bildschirm des Remotegeräts hervorheben, die die Benutzer überprüfen sollen. Sowohl Sie als auch Benutzer am Remotegerät sehen, was Sie mit dem Zeichentool auf dem Bildschirm machen. Die Zeichnungen werden auf beiden Bildschirmen angezeigt, bis Sie auf den Radiergummi in der Tool-Palette klicken.

Es stehen drei Zeichentools zur Auswahl:

- **Zeiger:** Mit dem Zeiger können Sie auf Objekte auf dem Bildschirm zeigen. Wenn Sie die linke Maustaste gedrückt halten, ist der Zeiger aktiv. Durch einen roten Punkt unter dem Mauszeiger kann der Benutzer sofort erkennen, wo sich der Zeiger befindet. Der Punkt wird ausgeblendet, sobald die linke Maustaste freigegeben wird. Die Farbe des Punktes ist nicht veränderbar. Der Punkt zieht, anders als der Bleistift, keine Spur.
- **Freihand:** Das Freihandtool verwenden Sie zum Zeichnen eines Pfeils, Einkreisen eines Objekts, Erstellen einer Freihandzeichnung usw. Mit dem Freihandtool sind Sie nicht an eine bestimmte Form gebunden.
- **Rechteck:** Mit diesem Tool können Sie ein Rechteck um ein Objekt auf dem Bildschirm zeichnen. Klicken Sie auf die Position, an der sich die Ecke des Rechtecks befinden soll. Ziehen Sie mit dem Mauszeiger, um ein Rechteck um den Bereich zu zeichnen, den Sie hervorheben möchten und lassen Sie dann die Maustaste los.

Außerdem können Sie Ihre Zeichnungen mithilfe der Dropdownlisten für die Linienstärke und die Linienfarbe verändern. Änderungen in diesen Einstellungen wirken sich nur auf neu gezeichnete Objekte aus. Wenn Sie mit dem Zeichnen fertig sind, klicken Sie auf den Radiergummi in der Zeichenpalette oder schließen Sie die Palette.

Anpassen von Remotesteuerungseinstellungen

Verwenden Sie im Dialogfeld **Extras > Optionen** die Registerkarte **Einstellungen ändern**, um die Remotesteuerungseinstellungen anzupassen.

- **Automatischen Bildlauf zulassen:** Aktiviert die Bildlauffunktion für das Viewer-Fenster, sobald Sie den Cursor näher an den Fensterrahmen verschieben. Je dichter Ihr Cursor an den Rand gelangt, umso schneller ist der Scrollvorgang.
- **Remotetastatur und -maus sperren:** Sperrt Tastatur und Maus des Remotegeräts, sodass nur die Person, die mit dem Viewer arbeitet, das Remotegerät bedienen kann. Beachten Sie, dass bestimmte Tastenkombinationen in Windows, beispielsweise Strg+Alt+Entf oder Windows-Taste+L, nicht gesperrt sind.
- **Zwischenablagen synchronisieren, um Inhalte zwischen Lokal- und Remotecomputern einfügen zu können:** Synchronisiert die Tastaturen des lokalen und des Remotegeräts, sodass Sie Informationen zwischen den beiden Geräten einfügen können.
- **Bildschirm des Remotecomputers ausblenden:** Blendet den Bildschirm des Remotegeräts aus, sodass nur die Person, die mit dem Viewer arbeitet, den Bildschirm auf dem Remotegerät einsehen kann.

- **Immer fragen, ob der Bildschirm des Remotecomputers beim Start der Remotesteuerung gelöscht werden soll:** Fragt den Remotebenutzer, ob es in Ordnung ist, dass sein Bildschirm während der Remotesteuerungssitzung gelöscht wird. Wenn diese Option ausgewählt ist, spielt es keine Rolle, ob die Option **Bildschirm des Remotecomputers ausblenden** aktiviert oder deaktiviert ist.
- **Remotecomputer sperren, wenn die Sitzung beendet wird:** Aktiviert nach Abschluss der Sitzung die Sperrfunktion des Betriebssystems. Hierdurch wird der Bediener der Remotesteuerung in die Lage versetzt, seine Arbeit abzuschließen und das System des Benutzers in einem sicheren Zustand zu hinterlassen, während der Benutzer nicht da ist oder bis er im Anschluss an eine Remotesteuerungssitzung seine Arbeit fortsetzen kann.
- **Automatische zugeordnete Tastatur:** Diese Option sollten Sie nicht deaktivieren. Sie ordnet die Tastatur des Zielgeräts neu zu, damit sie mit der des Administrators übereinstimmt. Damit wird sichergestellt, dass das, was der Administrator eingibt, korrekt auf dem Zielgerät angezeigt wird. Dies ist besonders nützlich, wenn die Administrator- und Zieltastaturen auf unterschiedlichen Alphabeten oder Sprachen basieren.
- **Kompatibilität mit alten Agenten (Agenten vor 8.5) aktivieren:** LANDesk hat die Remotesteuerungssicherheit geändert und in Version 8.5 einen neuen Remote Control Viewer hinzugefügt. Wenn es in Ihrem Netzwerk Remotesteuerungsagenten aus der Zeit vor Version 8.5 gibt, ermöglichen Sie dem neuen Remote Control Viewer durch Aktivieren dieser Option die Kommunikation mit diesen alten Agentenversionen.

Alternative Namen verwenden

Je nachdem, wie Sie den Remotesteuerungsagenten auf verwalteten Geräten konfiguriert haben, können Benutzer an einem Gerät, das aus der Ferne gesteuert wird, auf das Symbol für den Remotesteuerungsstatus in der Windows-Taskleiste doppelklicken und den Computernamen und Benutzernamen des Administrators anzeigen, der das Gerät aus der Ferne steuert. Wenn Sie aus Sicherheitsgründen verhindern möchten, dass Ihr wirklicher Computer- oder Benutzername von Remotegeräten aus sichtbar ist, können Sie einen alternativen Benutzer- und/oder Computernamen angeben, der im Dialogfeld "Remotesteuerungsstatus" auf Remotegeräten angezeigt wird.

So verwenden Sie alternative Namen

1. Klicken Sie auf **Extras > Optionen**.
2. Aktivieren Sie auf der Registerkarte **Einstellungen ändern** die Option **Alternative Namen benutzen**.
3. Geben Sie die Namen an, die für die Benutzer an Remotegeräten angezeigt werden sollen.
4. Klicken Sie auf **OK**.

Verwendung des Spiegeltreibers

Spiegeltreiber bieten mehrere Vorteile. Der Hauptvorteil liegt in einer durch Microsoft unterstützten Methode zur Erfassung der Bildschirmausgabe, ohne dass der bestehende Videotreiber modifiziert werden muss. Dadurch kann sich der Remotesteuerungs-Spiegeltreiber standardmäßig verhalten, sodass weniger Probleme bei den Geräten entstehen.

Der andere Vorteil liegt darin, dass der Spiegeltreiber nicht so viel Prozessorleistung des Zielgeräts konsumiert. Bei der Remotesteuerung von Geräten, die mit einem Prozessor von maximal 1,5 GHz ausgestattet sind, kann der Spiegeltreiber erhebliche Leistungsverbesserungen im Vergleich zu schnelleren Netzwerkverbindungen bringen. Bei langsameren Netzwerkverbindungen wird die Remotesteuerungsleistung mehr durch die Bandbreite als die Prozessorbelastung beeinflusst.

Der Standard-Remotesteuerungsagent wird immer auf den Geräten installiert. Wenn gleichzeitig ein Spiegeltreiber installiert wird, werden sowohl Standardagent als auch Spiegeltreiber unterstützt. Sie können den Standard-Remotesteuerungstreiber nicht deinstallieren und nur den Spiegeltreiber verwenden.

Ändern von Hotkey-Einstellungen für den Viewer

Der Remote Control Viewer unterstützt die folgenden Abkürzungstasten (**Extras > Optionen > Abkürzungstasten-Einstellungen**):

- **Abkürzungstasten aktivieren** (Strg+Alt+H): Aktiviert/Deaktiviert die Verfügbarkeit der Abkürzungstasten. Abkürzungstasten sind standardmäßig aktiviert.
- **Anzeigesitzung schließen** (Strg+Alt+S): Trennt die aktuelle Anzeigesitzung. Das Remote Control Viewer-Fenster bleibt geöffnet.
- **Strg+Alt+Entf senden** (Strg+Alt+D): Sendet Strg+Alt+Entf an das Zielgerät.
- **Remotetastatur und -maus sperren** (Strg+Alt+K): Aktiviert/Deaktiviert die lokale Maus und Tastatur des Zielgeräts
- **Vollbildmodus ein-/ausschalten:** (Strg+Alt+M): Wechselt auf dem Remote Control Viewer vom Fenstermodus in den Vollbildmodus und umgekehrt.
- **Strg+Esc senden** (STRG+Alt+E): Sendet Strg+Esc an das Zielgerät.
- **Maus- und Zeichenmodus-Umschaltung:** Schaltet zwischen Zeichenmodus und normalem Mauszeigermodus hin- und her.
- **An Bildschirmgröße anpassen**: Definiert eine Standard-Abkürzungstastenfolge zum Ein-und Ausschalten der Option An Bildschirmgröße anpassen.
- **Bildschirm aktualisieren:** Überträgt die Bildschirmdaten vom Remotecomputer neu.
- **Daten aktualisieren:** Sendet einen Befehl zum Aktualisieren (F5) an den Remotecomputer.
- **Sitzung trennen:** Beendet die aktuelle Remotesteuerungssitzung. Das Viewer-Fenster bleibt geöffnet.

Sie können einen Hotkey ändern, indem Sie in das Feld neben dem Hotkey klicken und die neue Tastenkombination drücken. Die Tasten "Bildschirm drucken" oder "Pause/Anhalten" dürfen nicht Teil einer Tastenkombination sein.

Senden von Strg+Alt+Entf an Vista- und Windows 7-Geräte

Die lokale Standardsicherheitsrichtlinie in Windows Vista und Windows 7 lässt Strg+Alt+Entf von einem Remote Control Viewer nicht zu. Sie können dies folgendermaßen ändern:

So erlauben Sie das Senden von Strg+Alt+Entf an Vista- und Windows 7-Geräte

1. Geben Sie im Suchfeld des **Start**menüs **gpedit.msc** ein und drücken Sie **Eingabe**.
2. Navigieren Sie zu **Lokale Computerrichtlinie > Administrative Vorlagen > Windows Komponenten > Windows Anmeldeoptionen > Software Secure Attention Sequence**.
3. Doppelklicken Sie auf **Software-SAS deaktivieren oder aktivieren**.

4. Klicken Sie auf **Aktiviert** und dann in Dropdownliste entweder auf **Dienste** oder **Dienste und Anwendungen für die erleichterte Bedienung**.
5. Klicken Sie auf **OK**.

Optimieren der Remotesteuerungsleistung

Verwenden Sie die Registerkarte **Leistung optimieren** des Dialogfelds **Optionen(Extras > Optionen)**, um die Remotesteuerungsleistung folgender Verbindungstypen zu optimieren:

- Langsame Verbindung (Modem)
- Mittelschnelle Verbindung (Broadband)
- Für schnelle Verbindung optimieren (LAN)
- Benutzerdefinierte Verbindung

Die Optimierung führt zu einer dynamischen Anpassung der folgenden Parameter: Farbreduzierung, Sichtbarkeit des Hintergrundbilds und Darstellung der Fenster auf dem Remotegerät (einstellbar über **Anzeige Eigenschaften > Darstellung > Effekte**), Übergangseffekte für Menüs und QuickInfo.

Zur Remotesteuerung von Daten wird immer ein hocheffizienter Kompressionsalgorithmus verwendet. Trotz Kompression müssen jedoch viele der Daten mit hoher Farbtiefe gesendet werden. Die Menge der zu sendenden Remotesteuerungsdaten kann durch Reduzierung der auf dem Remote Control Viewer angezeigten Farbtiefe erheblich verringert werden. Wenn der Viewer die Farbtiefe reduziert, muss er die volle Farbpalette vom remote gesteuerten Desktop einer reduzierten Farbpalette im Viewer zuordnen. Daher werden Farben im Remotesteuerungsfenster manchmal nicht genauso wie auf dem remote gesteuerten Desktop dargestellt. Falls dies ein Problem darstellt, sollte die Kompression auf eine höhere Qualität eingestellt werden.

Eine weitere Möglichkeit zur Leistungsoptimierung ist die Unterdrückung des Hintergrundbilds auf dem remote gesteuerten Gerät. In diesem Fall muss die Remotesteuerung keine Hintergrundbildaktualisierungen senden, wenn Teile des remote gesteuerten Desktops freigelegt werden. Hintergrundbilder benötigen oft eine hohe Bandbreite, z. B. wenn es sich um Fotos handelt. Diese lassen sich nicht gut komprimieren und brauchen bei langsameren Verbindungen lange für die Übertragung.

Die letzte Möglichkeit zur Leistungsoptimierung ist die Verwendung eines Spiegeltreibers auf dem Remotegerät. Weitere Informationen finden Sie unter "Verwendung des Spiegeltreibers" auf Seite 260.)

Interaktion mit Benutzern von remotegesteuerten Geräten

Bei einer Remotesitzung interagieren Sie direkt mit dem über die Remotesteuerungssitzung angesprochenen Endbenutzer bzw. dem Gerät selbst oder beidem. Mit dem Extra für die Remotesteuerung könne Sie ein Chatfenster aufrufen, Dateien übertragen, Programme auf dem Gerät ausführen oder das Gerät neu starten. Sie können ferner eine Aufzeichnung der Chatsitzung für sich als Referenz oder als Kopie für den Benutzer speichern.

Chat mit Remotegeräten

Verwenden Sie den Remote Control Viewer, um mit einem Benutzer zu chatten, der an einem Remotegerät sitzt. Diese Funktion ist dann hilfreich, wenn Sie einem Remotebenutzer Anweisungen geben müssen, dessen Wählverbindung die einzige verfügbare Telefonleitung verwendet. Der Benutzer kann über das Chatfenster antworten, das auf seinem Bildschirm angezeigt wird. Chatten können Sie nur auf Geräten, auf denen der Remotesteuerungsagent installiert ist. Diese Funktion ist auch dann verfügbar, wenn Sie den Bildschirm des Remotegeräts nicht einsehen.

Wenn Sie möchten, können Sie die Nachrichten einer Chatsitzung speichern. Der gesamte Text, der im grauen Bereich der Chatsitzung zu sehen ist, wird in einer Textdatei gespeichert.

So chatten Sie mit einem Benutzer an einem Remotegerät

1. Klicken Sie auf **Extras > Chat**. Ein Abschnitt des Viewer-Fensters wird als Chat-Bereich geöffnet.
2. Geben Sie im Abschnitt unten links des Chat-Bereichs eine kurze Nachricht ein. Klicken Sie auf **Senden**.

Ihre Nachricht wird in einem Chat-Fenster auf dem Bildschirm des Remotegeräts angezeigt. Der Benutzer kann antworten, indem er eine Nachricht eingibt und auf **Senden** klickt. Der Benutzer kann auch auf **Schließen** klicken, um die Chatsitzung zu beenden.

So speichern Sie Nachrichten aus einer Chatsitzung

1. Klicken Sie im Chatbereich des Ansichtsfensters auf **Speichern**.
2. Geben Sie einen Dateinamen im Dialogfeld **Speichern unter** ein und klicken Sie auf **Speichern**.

Übertragen von Dateien auf Remotegeräte

Verwenden Sie den Remote Control Viewer, um Dateien von und auf Ihren Computer an das Remotegerät zu übertragen. Dies funktioniert im Wesentlichen so, als ob Sie einem Remotegerät ein Laufwerk zugeordnet hätten. Sie können nur Dateien an Geräte bzw. von Geräten übertragen, auf denen der Remotesteuerungsagent installiert ist. Diese Funktion ist auch dann verfügbar, wenn Sie den Bildschirm des Remotegeräts nicht einsehen.

So übertragen Sie Dateien an ein Gerät

1. Klicken Sie auf **Extras > Dateiübertragung**. Der Windows Explorer wird angezeigt.
2. Wählen Sie eine zu übertragende Datei aus, indem Sie auf ihren Dateinamen klicken. Klicken Sie im Kontextmenü des Geräts auf **Kopieren**.
3. Blättern Sie in der Windows Explorer-Struktur nach unten, bis Sie zu LANDesk**Remotesteuerung** gelangen. Hier sollte der Name des Remotegeräts angezeigt werden, das Sie zur Zeit steuern.
4. Wählen Sie auf dem Remotegerät einen Ordner, in den die Datei eingefügt werden soll, klicken Sie mit der rechten Maustaste und klicken Sie auf **Einfügen**.

Auf gleiche Weise können Sie Dateien von einem Remotegerät auf Ihren Computer übertragen.

Ausführen von Anwendungen auf Remotegeräten

Sie können Programme auf Remotegeräten starten. Verwenden Sie das Feld "Ausführen" in der Viewer-Symbolleiste, um den Pfad und Dateinamen des Remoteprogramms einzugeben. Da das Programm auf dem Remotegerät gestartet wird, muss der von Ihnen eingegebene Pfad und Dateiname auf dem Remotegerät existieren.

So führen Sie ein Programm auf einem Remotegerät aus

1. Geben Sie im Feld **Ausführen** des Viewers den Pfad und Dateinamen für das auszuführende Programm ein. Wenn Sie weder den Pfad noch den Namen kennen, können Sie die Liste öffnen und auf **Durchsuchen** klicken. Damit wird ein Dialogfenster geöffnet, das es Ihnen gestattet, die Ordner des Remotegeräts zu durchsuchen.
2. Klicken Sie auf die Schaltfläche **Remoteausführung** rechts vom Feld **Ausführen**.

Neustart von Remotegeräten

Verwenden Sie den Remote Control Viewer, um über Remotezugriff einen Neustart auf einem Gerät durchzuführen. Sie können nur Geräte über Remotezugriff neu starten, auf denen der Remotesteuerungsagent installiert ist. Diese Funktion ist auch dann verfügbar, wenn Sie den Bildschirm des Remotegeräts nicht einsehen.

So werden Geräte über Remotezugriff neu gestartet

1. Klicken Sie auf **Extras > Neustart**.
2. Geben Sie im Bearbeitungsfeld **Timeout (Sekunden)** die Zeit ein, die einem Benutzer zur Verfügung steht, bevor der Gerät neu gestartet wird. Die maximale Verzögerung ist 300 Sekunden.
3. Geben Sie im Feld **Remotebenutzeraufforderung** eine kurze Warnung ein, die auf dem Bildschirm des Benutzers vor einem Remoteneustart angezeigt wird.
4. Sie können Ihre Einstellungen speichern, indem Sie auf **Diese Einstellungen speichern** klicken.
5. Klicken Sie auf **OK**.

Die Warnmeldung wird auf dem Gerät mit einem Countdown angezeigt, der zeigt, wie viel Zeit bis zum Neustart verbleibt. Der Benutzer hat die Möglichkeit, auf **OK** zu klicken, um sofort einen Neustart durchzuführen, oder er kann durch Klicken auf **Abbrechen** die Aktion abbrechen. Auf Ihrem Computer wird ein Meldungsfeld angezeigt, in dem Sie sehen können, ob der Benutzer die Anforderung abgebrochen hat. Wenn der Neustart durchgeführt wurde, sehen Sie eine Meldung im Sitzungsmeldungsbereich des Viewer-Fensters.

Ändern der Remotesteuerungssicherheit des Geräts

Management Suite kontrolliert Geräte in hohem Maße, wenn Zugriffsrechte erteilt werden. Das Gerät steuert die Remotezugriffssicherheit. Es speichert seine Sicherheitseinstellungen für den Remotezugriff in der Registrierung.

Sie können die Remotesteuerungseinstellungen und das Sicherheitsmodell auf Clients ändern, indem Sie die Einstellungen für die Agentenkonfiguration aktualisieren (**Extras > Agentenkonfiguration**) und vom Kontextmenü der aktualisierten Konfiguration aus auf **Aktualisierung planen** klicken. Sobald Sie die Aktualisierung auf Geräten bereitgestellt haben, benutzen die Geräteagenten die von Ihnen angegebenen Einstellungen.

Weitere Informationen finden Sie unter "Bereitstellen der Remotesteuerung" auf Seite 128.

Verwenden der Remotesteuerungsprotokollierung

Management Suite protokolliert standardmäßig Remotesteuerungsaktionen, einschließlich des Geräts, das remote gesteuert wird, und der Konsole, die die Remotesteuerung ausführt. Sie können die Remotesteuerungsprotokollierung deaktivieren oder Remotesteuerungsprotokolleinträge löschen, die älter als ein angegebenes Datum sind.

Wenn die Protokollierung aktiviert ist, können Sie die folgenden Remotesteuerungsberichte anzeigen (**Extras > Berichte/Überwachung > Berichte** und im Extra **Berichte** auf **Berichte > Standardberichte > Remotesteuerung** klicken):

- Remotesteuerungsverlauf nach Bediener:
- Remotesteuerungsübersicht
- (Die Liste der Standardberichte kann von Release zu Release variieren.)

So aktivieren oder deaktivieren Sie die Remotesteuerungsprotokollierung

1. Klicken Sie in der Management Suite Konsole auf **Konfigurieren > Remotesteuerungsprotokollierung**.
2. Aktivieren oder deaktivieren Sie je nach Präferenz die Option **Remotesteuerungsverlauf aktivieren**.

So löschen Sie den Inhalt des Remotesteuerungsprotokolls

1. Klicken Sie auf **Konfigurieren > Remotesteuerungsprotokollierung**.
2. Geben Sie das Datum ein, das Sie löschen möchten. Alle Einträge, die älter sind als dieses Datum, werden gelöscht.
3. Klicken Sie auf **Verlauf löschen**, um die Einträge aus dem Protokoll zu löschen.

Wenn verwaltete Geräte das Remotesteuerungsmodell "Windows NT-Sicherheit" verwenden, sind einige zusätzliche Schritte erforderlich, um sicherzustellen, dass in den Remotesteuerungsberichten die richtigen Informationen angezeigt werden. Unter dem Modell "Windows NT-Sicherheit" müssen sowohl Remotesteuerungsoperator als auch verwaltete Geräte Mitglieder derselben Windows-Domäne sein. Darüber hinaus müssen Sie sicherstellen, dass sich die Domänenkonten für alle Remotesteuerungsoperatoren in der Gruppe **Remotesteuerungsoperatoren** auf der Agentenkonfigurationsseite **Remotesteuerung** befinden. Wenn Sie diese Schritte nicht ausführen, zeigt der Remotesteuerungsbericht den lokalen Benutzer als den Remotesteuerungsoperator anstatt als den eigentlichen Operator an.

Aktivierung der Remotesteuerungsprotokollierung in eine Textdatei

Sie können die Remotesteuerungsprotokollierung in eine Textdatei aktivieren, indem Sie auf verwalteten Geräten die folgenden Registrierungsschlüssel erstellen:

- Erstellen Sie den folgenden DWORD-Wert und setzen Sie ihn auf 1: HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\Container\LogSessionMessages.
- Erstellen Sie den folgenden Zeichenfolgewert und setzen Sie diesen auf einen UNC-Pfad (einschließlich vorangestelltem umgekehrten Schrägstrich): HKLM\SOFTWARE\LANDesk\Instant Support Suite Console\LogPath.

Der Dateiname für das Protokoll lautet issuser.log.

Ändern des Remotesteuerungsmodus auf Zielgeräten

Der LANDesk Remotesteuerungsagent akzeptiert zwei Verbindungstypen auf Geräten:

- Direkte Verbindungen vom LANDesk Remote Control Viewer-Fenster.
- Management Gateway-Verbindungen über ein Management-Gateway.

Der Remotesteuerungsagent wartet nur auf einen Verbindungstyp. Wenn Sie den Verbindungstyp, auf den der Agent wartet, ändern möchten, doppelklicken Sie auf das Symbol für den Remotesteuerungsstatus in der Taskleiste des Zielgeräts und klicken Sie auf **Modus wechseln**. Hiermit schaltet der Agent zwischen dem direkten Modus und dem Gateway-Modus um. Text im Dialogfeld "Remotesteuerungsstatus" zeigt, welcher Modus zurzeit auf dem Remotesteuerungsagent aktiviert ist. Sie können entweder den Benutzern die Möglichkeit geben, den Moduswechsel selbst vorzunehmen oder Sie können dies im Rahmen einer Remotesteuerungssitzung selbst veranlassen. Wenn Sie den Modus im Rahmen einer Remotesteuerungssitzung wechseln, wird die Sitzung getrennt, sobald Sie auf die Schaltfläche **Modus wechseln** klicken.

Der LANDesk System Manager unterstützt den Management Gateway nicht, daher erscheint diese Schaltfläche immer blass auf Geräten, die vom System Manager verwaltet werden.

Anpassen des Viewers und der Remotesteuerungsagenten

Der Remote Control Viewer verfügt über Befehlszeilenoptionen, mit denen seine Funktionen angepasst werden können. Falls nötig, können sogar die Registrierungsschlüssel der Remotesteuerungsagenten auf Geräten angepasst werden. Normalerweise werden diese Registrierungsschlüssel von der Konfiguration des Remotesteuerungsagenten festgelegt, die Sie auf Geräten bereitstellen.

Befehlszeilenoptionen für den Viewer

Der Remote Control Viewer kann mithilfe einer Befehlszeilenoption gestartet werden, die sofort ein Viewer-Fenster öffnet, eine Verbindung zu einem bestimmten Gerät herstellt und die gewünschten Viewer-Funktionen aktiviert, wie z. B. Remotesteuerung, Chat, Dateiübertragung oder Neustart des Geräts. Das Remotesteuerungsprogramm isscntr.exe befindet sich im ManagementSuite-Programmordner.

Die Remotesteuerungs-Befehlszeilenoptionen haben folgende Syntax:

```
isscntr /a<address> /c<command> /l /s<core server>
```

Falls Ihr Coreserver zertifikatbasierte oder integrierte Sicherheit zur Remotesteuerung verwendet, müssen Sie den /s-Parameter verwenden, um den Coreserver anzugeben.

Option	Beschreibung
/a<address>	Verbindung mit einem Gerät an einer bestimmten TCP/IP-Adresse aufnehmen. Die TCP/IP-Adresse kann sowohl numerische Adressen als auch Namen als Adressen enthalten, die durch Strichpunkte getrennt sind. Außerdem können Sie den Hostnamen angeben.
/c<command>	Starten Sie den Remote Control Viewer und führen Sie eine Funktion aus. (Siehe unten unter "Befehlsnamen".) Sie können mehrere /c Argumente in der Befehlszeile eingeben. Zum Beispiel: isscntr /agamma /c"remote control" /c"file transfer" Die folgenden Funktionen stehen zur Auswahl. **Remotesteuerung**: Öffnen eines Remotesteuerungsfensters

Option	Beschreibung
	Neustart: Neustart eines Geräts **Chat**: Öffnen eines Chat-Fensters **Dateiübertragung**: Öffnen einer Dateiübertragungssitzung **Systeminfo**: Öffnen eines Fensters, in dem Informationen über das Gerät angezeigt werden, wie Betriebssystem, Arbeitsspeicher und verfügbarer Speicherplatz auf der Festplatte.
/l	Einschränkung der Viewer-Benutzeroberfläche, sodass nur die Funktionen angezeigt werden, die Sie mit /c angeben.
/s<core server>	Wenn Sie die zertifikatbasierte Sicherheit verwenden, geben Sie mit dieser Option den Coreserver für die Authentifizierung an. Diese Option ist nützlich, wenn Sie in einer Umgebung mit mehreren Cores Clients remote steuern. Falls Ihr Coreserver zertifikatbasierte oder integrierte Sicherheit zur Remotesteuerung verwendet, müssen Sie den /s-Parameter verwenden, um den Coreserver anzugeben.

Beispiel 1

Öffnet das Viewer-Fenster. Alle Änderungen (wie z. B. eine Größenanpassung des Fensters mit Verbindungsmeldungen oder Änderungen der Leistungsoptionen) bleiben von der letzten Verwendung des Viewer-Fensters erhalten.

```
isscntr
```

Beispiel 2

Startet eine Remotesteuerungssitzung mit dem Gerät "gamma". (Beachten Sie, dass es zwischen "/a" und "gamma" kein Leer- oder Interpunktionszeichen gibt.)

```
isscntr /agamma /c"remote control"
```

Beispiel 3

Start einer Remotesteuerungssitzung und Chat-Sitzung; Verbindungsherstellung zu einem Gerät mit dem Namen "gamma". Die Remotesteuerung versucht zuerst, den Namen "gamma" zu finden. Sollte dies fehlschlagen, wird versucht, eine Verbindung zu der numerischen Adresse 10.10.10.10 herzustellen:

```
isscntr /agamma;10.10.10.10 /c"remote control" /c"chat"
```

Beispiel 4

Port 9535 wird zur Kommunikation zwischen Viewer und Agentencomputern verwendet. Wenn Geräte, auf denen issuser.exe ausgeführt wird, für einen anderen Port als den Port 9535 konfiguriert wurden, muss der Port als Teil der an isscntr.exe übergebenen Adresse angegeben werden. Beispiel: Zur Remotesteuerung eines Geräts mit der Adresse 10.4.11.44 bei dem issuser32.exe zur Verwendung von Port 1792 als Verifizierungsport konfiguriert ist, würde die Befehlszeile so aussehen:

```
isscntr /a10.4.11.44:1792 /c"remote control"
```

Beheben von Fehlern in Remotesteuerungssitzungen

Dieser Abschnitt beschreibt mögliche Probleme bei der Remotesteuerung eines Geräts und liefert mögliche Lösungen.

Ich kann ein Gerät nicht remote steuern

Überprüfen Sie, ob auf dem Gerät die LANDesk Agenten geladen sind.

So überprüfen Sie, ob die LANDesk Agenten geladen sind

- Klicken Sie in der Netzwerkansicht der Konsole auf **Eigenschaften** im Kontextmenü des Geräts. Klicken Sie auf die Registerkarte **Agenten** und zeigen Sie die geladenen Agenten an.

So laden Sie den Remotesteuerungsagent

- Erstellen Sie einen Agenten-Konfigurationstask in der Konsole und verteilen Sie ihn mittels Pushvorgang auf das Gerät. Alternativ dazu können Sie auch ein Laufwerk auf dem Gerät dem Coreserver zuordnen und den entsprechenden Gerätekonfigurationstask ausführen.

Kann keine Dateien zwischen Konsole und Zielgerät übertragen

Überprüfen Sie, ob Norton AntiVirus ausgeführt wird und ob Integrity Shield aktiviert ist. Wenn Integrity Shield aktiviert ist, benötigen Sie vorübergehende Rechte, um in das Verzeichnis kopieren zu können, das von Integrity Shield geschützt wird.

Soft-
ware-
verteilung/Verteilungspakete/Verteilungsmethoden

Informationen zur Softwareverteilung

Die Softwareverteilungstechnologie in LANDesk Management Suite unterstützt das IT-Personal bei der Implementierung einer kontrollierten Automatisierung für eine schnelle und effiziente Verteilung und Installation von Software, für Sicherheits- und Antivirusupdates sowie für das Anwendungspatchmanagement in heterogenen Netzwerkumgebungen. Die Technologie baut auf einem modularen, taskorientierten Modell auf, das wesentlich zur Steigerung der Effizienz bei der Vorbereitung, Planung und Verwaltung von Softwareverteilungen insgesamt beitragen kann. Pakete, Verteilungsmethoden, Bereitstellungsskripts und Zielauswahl werden separat verwaltet, um die Flexibilität insgesamt zu steigern.

Wesentliche Funktionen und Vorteile

- **Rückgabecodezuordnungen:** Definition von Rückgabecodes zur Verbesserung der Genauigkeit der Anwendungsinstallation.
- **Native MSI-Unterstützung:** Kopieren und Einfügen von MSI-Befehlszeilenaufrufen.
- **Vereinfachter Workflow:** Einfachere und schnellere Planung von Paketinstallationen.
- **Vereinfachte Bandbreitensteuerung:** Sachgerechte individuelle Anpassung von Konfigurationen.
- **Taskbasierte Modellierung:** Effizienzsteigerung dank Trennung von Paketerstellungs- und -verteilungsmethoden.
- **LANDesk® Targeted Multicast™: Verteilung** großer Pakete an mehrere Benutzer mit minimalem Bandbreitenbedarf und ohne dedizierte Hardware- oder Routerkonfigurationen.
- **LANDesk® Peer Download™:** Zugriff auf Pakete, die bereits an ein Subnetz ausgeliefert wurden.
- **Voraussetzungsüberprüfung und Paketverkettung:** Installation vorausgesetzter Pakete und die Möglichkeit, mehrere Pakete automatisch in einen einzigen Arbeitsgang zu installieren.
- **Taskplaner:** Vereinfachung der Zielauswahl dank Integration in Verzeichnisdienst und Assetinventar-Datenbanken.
- **Paketagnostische Verteilung:** Bereitstellung beliebiger Pakettypen und Zugriff auf MSI-Unterstützung.für mehrere Dateien.
- **Self-Service-Portal:** Reduzierung der Anzahl der Helpdesk-Incidents, Initiierung genehmigter Installationen durch die Benutzer und schnellere Fehlerbehebung dank ausführlicher Verlaufsdaten.
- **Richtlinienbasierte Verteilung:** Bereitstellung mehrerer Softwarepakete in einer einzigen Richtlinie und Sicherstellung der Verfügbarkeit der Pakete für zukünftige Updates und eine erneute Anwendung, falls erforderlich.

Die Softwareverteilung bei Management Suite umfasst die folgenden Hauptschritte:

1. **Erstellen oder Abrufen eines Softwarepakets**. Das Softwarepaket kann aus einer oder mehreren MSI-Dateien, einer ausführbaren Datei, einer Batchdatei, einem Macintosh- oder Linux-RPM-Paket, einem Windows Script Host-Paket, einem Application Virtualization-Paket oder einem mit dem Legacy-Package Builder von Management Suite erstellten Paket bestehen. Kopieren Sie das Paket auf Ihren Delivery-Server.

2. **Erstellen eines Verteilungspakets (Extras > Verteilung > Verteilungspakete)**. Das Verteilungspaket enthält die Dateien und Einstellungen, die erforderlich sind, um ein bestimmtes Softwarepaket zu installieren (beispielsweise der Paketname, alle etwaigen Abhängigkeiten oder Anforderungen, Befehlszeilenparameter, zusätzlich zu installierende Dateien usw.). Diese Einstellungen werden in der Datenbank gespeichert und bilden ein Verteilungspaket. Nachdem Sie ein Verteilungspaket erstellt haben, werden die Informationen in der Datenbank gespeichert und lassen sich problemlos in mehreren Tasks verwenden.
3. **Definieren einer Verteilungsmethode (Extras > Verteilung > Verteilungsmethode)**. Die Verteilungsmethode bestimmt, wie das Paket an die Geräte gesendet wird. Diese Optionen sind nicht mit einem bestimmten Verteilungspaket verknüpft. Die Optionsauswahl umfasst Targeted Multicast- und Push- und/oder richtlinienbasierte Verteilungen. Definieren Sie nicht jedes Mal, wenn Sie ein Paket verteilen möchten, eine Verteilungsmethode. Verteilungsmethoden bieten Ihnen die Möglichkeit, bewährte Verfahren für die Softwarebereitstellung zu definieren. Idealerweise erstellen Sie eine Vorlage für Liefermethoden, die sich für Verteilungen, bei denen dieselbe Verteilungsmethode zum Einsatz kommt, erneut verwenden lässt.
4. **Planen des Verteilungsauftrags im Fenster "Geplante Tasks" (Extras > Verteilung > Geplante Tasks)**. Sie geben das Verteilungspaket, die Verteilungsmethode und die Geräte an, an die das Verteilungspaket übermittelt werden muss, und legen den Zeitpunkt für die Ausführung des Tasks fest.
5. Zur geplanten Zeit startet der Planerdienst den Handler für den geplanten Task; der Handler stellt das Paket unter Verwendung der Optionen bereit, die in der Verteilungsmethode ausgewählt wurden. Hierzu zählen folgende:

    - Wenn eine Verteilungsmethode, die Multicast verwendet, ausgewählt wird, wird Multicast verwendet.
    - Wenn eine Push-Verteilungsmethode ausgewählt ist, kontaktiert der Dienst den Softwareverteilungsagenten auf dem jeweiligen Gerät und teilt ihm mit, dass das Paket installationsbereit ist.
    - Wenn eine richtlinienbasierte Verteilungsmethode ausgewählt wurde, wird das Paket für den Download zur Verfügung gestellt.

6. Der Softwareverteilungsagent lädt das Paket aus seinem lokalen Cache, einem Peer im Netzwerk oder dem Delivery-Server und bearbeitet es auf dem Gerät, indem er die verpackten Dateien installiert oder entfernt.
7. Sobald die Paketverarbeitung abgeschlossen ist, sendet der Softwareverteilungsagent das Ergebnis an den Coreserver, wo es in die Coredatenbank geschrieben wird.

Die Trennung der Verteilungstasks in zwei Bereiche (Verteilungspakete und Verteilungsmethoden) vereinfacht den Verteilungsvorgang. Jetzt können Sie Vorlagen für Verteilungsmethoden erstellen, die von keinem bestimmten Paket abhängig sind. Beispiel: Sie könnten eine Standardvorlage für die Targeted Multicast-Verteilungsmethode erstellen und dann jedes Mal, wenn Sie eine Multicast-Verteilung durchführen möchten, das Paket mithilfe dieser Vorlage liefern, ohne das Verteilungspaket oder die Verteilungsmethode neu konfigurieren zu müssen.

Wenn in Ihrem Unternehmen mehrere Personen Pakete erstellen und verteilen, helfen diese Änderungen, die Jobfunktionen und Aufteilung des Tasks zu vereinfachen. Benutzer, die Pakete erstellen, sind damit von den Paket-Verteilungsmethoden unabhängig.

Grundlegendes zu Verteilungspakettypen

Die Softwareverteilung unterstützt folgende Pakettypen:

MSI

Diese Pakete liegen im Windows Installer-Format vor. Die MSI-Pakete müssen mit dem Tool eines Drittanbieters erstellt werden. Diese Pakete bestehen aus einer primären .msi-Datei und können unterstützende Dateien und Transformationen enthalten. Mit den "Transformationen" können Sie festlegen, wie MSI-Pakete erstellt werden. Wenn Ihr MSI-Paket aus mehreren Dateien besteht, sollten Sie sicherstellen, dass Sie alle Dateien in das Dialogfeld **Verteilungspaket** einfügen.

Ausführbare Datei

Damit ein ausführbares Paket von der Softwareverteilung verwendet werden kann, muss es folgende Kriterien erfüllen:

- Das ausführbare Paket darf nicht beendet werden, bevor die Installation abgeschlossen ist.
- Das ausführbare Paket muss Null (0) für eine erfolgreiche Installation zurückgeben.

Solange das ausführbare Paket diese beiden Bedingungen erfüllt, kann jede ausführbare Datei zum Installieren des Pakets verwendet werden. Sie können zusätzliche Dateien für ausführbare Pakete einschließen.

Batchdatei

Batchdatei-Pakete basieren auf einer Windows/DOS-Batchdatei. Sie können zusätzliche Dateien für diese Verteilungspakete einschließen. Der Status bei einem erfolgreichen Abschluss der Batchdatei-Paketausführung basiert auf dem Wert der errorlevel-Systemumgebungsvariable, nachdem die Batchdatei vollständig ausgeführt wurde.

Macintosh

Es kann jede beliebige Macintosh-Datei heruntergeladen werden, Verzeichnisse werden mit Management Suite jedoch nicht heruntergeladen. Installationspakete (.pkg) können Verzeichnisse enthalten. Sie müssen komprimiert sein. Wenn die heruntergeladene Datei über die Erweiterung .sit, .zip, .tar, .gz, .sea, oder .hqx verfügt, wird die Datei von Management Suite vor dem Zurückkehren dekomprimiert. (Benutzer müssen sich vergewissern, dass in Stuffit Expander die Option zum Suchen nach neuen Versionen deaktiviert ist. Andernfalls wird die Skriptausführung u. U. durch ein Dialogfeld unterbrochen.)

Linux-RPM

Diese Pakete liegen im Linux-RPM-Format vor. Diese Pakete müssen in einer Webfreigabe gespeichert sein, damit die Linux-RPM-Verteilung funktioniert.

LANDesk Application Virtualization

LANDesk Application Virtualization virtualisiert Anwendungen mithilfe der Thinstall-Technologie, wobei die virtualisierten Dateien zusammen mit der Anwendung und mit den .DLL/Gerätetreiberabhängigkeiten in eine einfache, unabhängige EXE-Datei gepackt werden. Die virtualisierten Anwendungen werden in einer isolierten Umgebung ausgeführt, ohne die Windows-Installation zu ändern, unter der sie ausgeführt werden.

Virtualisierte Anwendungen laufen auf Geräten mit gesperrter Konfiguration ("Locked-Down"-PCs), ohne dass hierzu zusätzliche Berechtigungen erforderlich sind.

Virtualisierte Anwendungen bestehen im Allgemeinen aus einer oder aus mehreren EXE-Dateien. Die ausführbaren Dateien einer virtualisierten Anwendung können mithilfe der Softwareverteilung auf verwalteten Geräten bereitgestellt werden. Pakete mit virtualisierten Anwendungen können mit jeder der verfügbaren Softwareverteilungsmethoden verteilt werden, auch durch Ausführung des Run-Befehls von der Quelle aus. Wenn Sie ein virtualisiertes Anwendungspaket mit der Option "Ausführung von Quelle" bereitstellen, verwenden die verwalteten Geräte eine Programmverknüpfung, um die EXE-Datei der virtualisierten Anwendung über das Netzwerk auszuführen.

Windows Script Host Package (.wsf)

Windows Script Host Packages (WSH) sind die als Alternative zu Batchdateien verwendete, neue Methode von Microsoft Software, die häufig zur Automatisierung vergleichbarer Tasks eingesetzt wird, wie zum Beispiel der Zuordnung von Laufwerken, dem Kopieren von Dateien oder der Änderung von Registrierungsschlüsseln. Die WSH-Dateien werden meistens in Verbindung mit Jscript (.js) und VBScript (.vbs) verwendet. Ein entscheidender Vorteil, den das Windows Script Host-Paket gegenüber dem .bat-Paket für Benutzer bietet, ist die Möglichkeit, mehrere Sprachen unter Verwendung der sprachunabhängigen Dateierweiterung (.wsf) in eine einzige Datei zu kombinieren. Diese Pakete können zumeist in einem Texteditor, HTML-Editor, Microsoft Visual C++ oder Visual InterDev erstellt werden.

SWD-Paket

Diese Pakete werden mit dem Legacyprogramm LANDesk Enhanced Package Builder (separat installiert) zusammengesetzt. Auch wenn Enhanced Package Builder nicht mehr im Lieferumfang von Management Suite enthalten ist, bietet LANDesk Software weiterhin Unterstützung für die Verteilung von Dateien, die mit diesem Programm erstellt wurden. Es handelt sich hierbei um ausführbare Dateien mit Eigenschaften, die sie eindeutig als Softwareverteilungspakete (SWD-Pakete) kennzeichnen.

Grundlegendes zu den verfügbaren Verteilungsmethoden

Die Softwareverteilung stellt folgende Verteilungsmethoden zur Verfügung:

- **Push:** Die Pakete können per Multicast auf die verwalteten Geräte übertragen werden. Der Coreserver initiiert dann die Paketinstallation auf den verwalteten Geräten.
- **Richtlinie:** Der Coreserver stellt die Pakete für den Download zur Verfügung. Wenn ein verwaltetes Gerät nach verfügbaren Richtlinien sucht, wird das Paket zurückgegeben. Je nach Richtlinientyp können die Geräte das Paket automatisch installieren oder das Paket Benutzern zur Verfügung stellen, damit sie es jederzeit installieren können.
- **Richtlinienbasierter Push:** Die kombinierte Pushverteilung und das Richtlinienmodell. Zuerst versucht die Softwareverteilung, das Paket auf allen Geräten in der Zielliste zu installieren. Auf diese Weise können Sie eine erstmalige Bereitstellung mittels Targeted Multicast durchführen. Im zweiten Schritt erhalten alle Geräte, auf denen das Paket nicht angekommen ist oder die erst später zur Zielliste hinzugefügt wurden (beispielsweise im Fall einer dynamischen Zielliste), das Paket, wenn der richtlinienbasierte Verwaltungsagent auf dem Gerät das Paket anfordert. Die ist die im Allgemeinen empfohlene Verteilungsmethode.
- **Multicast (nur Cache):** Überträgt das Paket per Multicast auf die Zielgeräte; es werden keine anderen Aktionen auf dem verwalteten Gerät veranlasst. Dieser Vorgang bewirkt, dass das Paket auf verwalteten Geräten lokal zwischengespeichert wird. Mit dieser Option kann das Paket via Multicast an einzelne Geräte in jeder Multicast-Domäne verteilt werden. Anschließend können Sie einen Task erstellen, der die Option **Peerdownload (nur vom Cache oder Peer installieren)** verwendet. Hiermit können Sie die für die Verteilung benutzte Netzwerkbandbreite regulieren, sodass sie sich auf Multicast-Domänen erstreckt.

HINWEIS: LANDesk stellt für jeden dieser Verteilungsmethodentypen Standardkonfigurationen für Verteilungsmethoden bereit. Die in diesen Standardmethoden definierten Standardeinstellungen sollten in den meisten Umgebungen gut funktionieren. Wenn Sie eine dieser Standardmethoden ändern möchten, sollten Sie mit Kopieren und Einfügen ein Duplikat der Verteilungsmethode erstellen und dieses umbenennen, um die Standardwerte in der Originaldatei für den zukünftigen Gebrauch zu bewahren.

Einrichten eines URL-basierten Delivery-Servers für die Softwareverteilung

Der Delivery-Server (Server für die Verteilung von Paketen) ist der Server, auf dem Softwareverteilungspakete gespeichert werden. Dabei kann es sich entweder um einen Webserver oder einen Windows-Dateiserver handeln. Zur Erzielung eines optimalen Ergebnisses sollten die Pakete URL-basiert sein. Im Allgemeinen ist das korrekte Konfigurieren einer URL weniger aufwendig als das Konfigurieren eines UNC-Pfads.

Auf HTTP-Paketfreigaben müssen Internet-Gästekonten mit mindestens Leseberechtigung hinzugefügt sein, weil auf die Pakete über anonymes HTTP zugegriffen wird.

So konfigurieren Sie einen Webserver für die Softwareverteilung

In den folgenden Schritten wird beschrieben, wie ein virtuelles Verzeichnis auf einem Webserver erstellt und für Suchvorgänge aktiviert wird. Im Allgemeinen gilt, dass sich virtuelle Verzeichnisse lesen und durchsuchen lassen müssen. Des Weiteren muss der anonyme Zugriff auf das virtuelle Verzeichnis aktiviert sein. Die Berechtigung zum Ausführen darf nicht aktiviert sein, weil die Freigabe sonst nicht einwandfrei arbeitet. Außerdem sollten Sie Schreibberechtigungen deaktivieren, damit Geräte den Verzeichnisinhalt nicht ändern können.

1. Erstellen Sie ein Verzeichnis auf dem Webserver, in dem die Softwareverteilungspakete gespeichert werden sollen. Im Normalfall wird dafür auf einem IIS-Webserver ein Unterverzeichnis des Verzeichnisses c:\inetpub\wwwroot verwendet.
2. Kopieren Sie die Pakete in dieses Verzeichnis.
3. Doppelklicken Sie in der Systemsteuerung auf **Verwaltung** und anschließend auf **Internetdienste-Manager**.
4. Doppelklicken Sie im rechten Bereich auf das Symbol mit dem Namen des Geräts und klicken Sie dann auf **Standardwebsite**.
5. Klicken Sie im rechten Bereich mit der rechten Maustaste auf eine freie Stelle, wählen Sie **Neu** und klicken Sie auf **Virtuelles Verzeichnis**.
6. Klicken Sie im Assistenten auf **Weiter** und geben Sie einen Alias für das Verzeichnis ein. Klicken Sie auf **Weiter**.
7. Geben Sie den Pfad ein oder wechseln Sie zum gewünschten Pfad und klicken Sie auf **Weiter**.
8. Aktivieren Sie im Dialogfeld "Zugriffsberechtigungen" die Optionen **Skript ausführen** und **Durchsuchen**. Auf diese Weise können Sie Pakete beim Erstellen eines Verteilungspakets durchsuchen. Klicken Sie auf **Weiter** und auf **Fertigstellen**.
9. Klicken Sie im Kontextmenü des soeben von Ihnen erstellten virtuellen Verzeichnisses auf **Eigenschaften**.

10. Löschen Sie auf der Registerkarte **Dokumente** die Option **Standardinhaltsseite aktivieren** und klicken dann auf **OK**. Die Standardseiten können die Fähigkeit der Freistellung beeinträchtigen, ein navigierfähiges Verzeichnis bereitzustellen.
11. Klicken Sie auf der Registerkarte **Verzeichnis Sicherheit** im Feld **Authentifizierungs- und Zugriffssteuerung** auf **Bearbeiten**. Achten Sie darauf, dass **Integrierte Windows-Authentifizierung** aktiviert ist. Beachten Sie außerdem, dass **Digest-Authentifizierung für Windows-Domänenserver** deaktiviert ist.
12. Um **Anschluss 80** auf dem Webserver zu aktivieren, klicken Sie im linken Bereich mit der rechten Maustaste auf **Standardwebsite**.
13. Klicken Sie auf **Eigenschaften**. Im Dialogfeld **Identifikation der Webseite** muss im Feld **TCP-Anschluss** der Wert 80 angezeigt werden. Andernfalls müssen Sie auf **Erweitert** klicken, um den Anschluss hinzuzufügen.
14. Stellen Sie sicher, dass die Website verfügbar ist, indem Sie einen Browser öffnen und die URL des Webservers sowie ein virtuelles Verzeichnis eingeben. Wenn der Webserver "Test" heißt und der Name des virtuellen Verzeichnisses "Pakete" lautet, geben Sie folgenden URL ein:

    http://Test/Packages

    Eine Liste der Pakete, die in dieses Verzeichnis kopiert wurden, wird angezeigt.

Sofern der Speicherplatz der Festplatte dies zulässt, können Sie Pakete in beliebiger Größe und Anzahl in diesem Verzeichnis speichern. Mithilfe von Unterverzeichnissen können Pakete logisch gruppiert werden. Für jedes Unterverzeichnis, das erstellt wird, muss die Zugriffsberechtigung entsprechend der obigen Beschreibung zum Task "So konfigurieren Sie einen Webserver für die Softwareverteilung" eingestellt sein.

Sobald Sie die Pakete in die Paketfreigabe eines Webservers kopiert haben, werden sie bereitgestellt und können auf die Zielgeräte kopiert werden. Zum geplanten Zeitpunkt wird die URL oder der UNC-Pfad des Pakets als Befehlszeilenparameter an SDClient.exe (den Geräteagent) übergeben. SDClient.exe verwaltet die Dateiübertragung, startet die Installation und erstellt Statusberichte. Für die Dateiübertragung wird zwar das HTTP-Protokoll verwendet, der Statusbericht wird jedoch über den Standard LANDesk Agent zurückgegeben.

Der Webserver kommuniziert mit dem Gerät, um sicherzustellen, dass das Paket fehlerfrei kopiert wird. Wenn die Paketübertragung während des Downloads unterbrochen wird, kann der Webserver den Download mithilfe des HTTP-Protokolls an der Stelle fortsetzen, an der er unterbrochen wurde. Der Webserver überprüft jedoch nicht, ob das Paket richtig installiert wurde. Dieser Verkehr basiert auf TCP und der Status wird mithilfe des Standard LANDesk Agent an den Coreserver zurückgegeben.

Konfigurieren eines IIS-Webservers für die Softwareverteilung

Beim Bereitstellen von Paketen auf einem Microsoft IIS-Webserver müssen zusätzlich folgende Konfigurationsschritte ausgeführt werden:

- Konfigurieren des virtuellen Verzeichnisses, das als Host für Ihre Pakete verwendet wird
- Registrieren eines MIME-Typs mit IIS.

IIS 6 handhabt virtuelle Verzeichnisse anders als IIS 5 (IIS 5 war der Windows 2000 Webserver). Wenn Sie auf einem IIS 6-Server ein Verzeichnis auswählen und es in dessen Kontextmenü als Web-Freigabe konfigurieren, registriert sich das Verzeichnis in IIS 6 als eine Webanwendung, nicht als ein virtuelles Verzeichnis. Problematisch an der Registrierung als Webanwendung ist hierbei, dass der Webserver bei der Auswahl einer ausführbaren Datei versucht, die Datei als Webanwendung auszuführen, statt sie auf das System des Benutzers downzuloaden.

Die Lösung besteht darin, das freigegebene Verzeichnis im IIS von einer Webanwendung in ein virtuelles Verzeichnis zu ändern und die Berechtigungen zum Ausführen zu deaktivieren.

Beim Hosten von Dateien auf einem IIS 6-Server verursachen Dateien ohne registrierten MIME-Dateityp einen HTTP-Fehler 404, "File Not Found" (Datei nicht gefunden). Dies führt zu einer Fehlermeldung beim Multicasting oder Installieren der Datei, es sei denn, Sie registrieren MIME-Dateitypen.

So registrieren Sie MIME-Dateitypen

1. Starten Sie den Internet Information Services (IIS)-Manager.
2. Erweitern Sie den lokalen Computer in der Strukturansicht.
3. Klicken Sie auf **Websites > Standardwebsite**.
4. Klicken Sie im Kontextmenü der Webfreigabe, die das Paket enthält, auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **HTTP-Header**.
6. Klicken Sie auf **MIME-Typen**.
7. Klicken Sie auf **Neu**.
8. Geben Sie im Feld **Erweiterung** ein Sternchen (.*) ein.
9. Geben Sie im Feld **MIME-Typ** Folgendes ein: **application/octet-stream**.
10. Doppelklicken Sie auf **OK** und übernehmen Sie die Änderungen.

Einrichten eines UNC-basierten Delivery-Servers für die Softwareverteilung

Der Delivery-Server (Server für die Verteilung von Paketen) ist der Server, auf dem Softwareverteilungspakete gespeichert werden. Dabei kann es sich entweder um einen Webserver oder einen Windows-Dateiserver handeln. Zur Erzielung eines optimalen Ergebnisses sollten die Pakete URL-basiert sein. Im Allgemeinen ist das korrekte Konfigurieren einer URL weniger aufwendig als das Konfigurieren eines UNC-Pfads.

Auf UNC-Paketfreigaben müssen Domänen-Computergruppen mit mindestens Leseberechtigung hinzugefügt sein.

Geräte, die keinen Browser besitzen, müssen Verteilungspakete über einen UNC-Pfad auf einem Windows-Netzwerkserver erhalten. Dazu kann derselbe Ordner verwendet werden, den Sie auf Ihrem Webserver eingerichtet hatten. Wenn Sie bevorzugte Server verwenden, können Sie die Authentifizierungsnachweise für Ihre UNC-Paketfreigabe dort konfigurieren, ohne eine Null-Session-Freigabe konfigurieren zu müssen.

Wenn Sie keine bevorzugten Server oder bevorzugten Servernachweise verwenden, müssen Sie Ihre Paketfreigaben-Null-Session erstellen, was es den Benutzern erlaubt, ohne Eingabe alternativer Nachweise auf die Freigabe zuzugreifen. Verwenden Sie das Dienstprogramm SysShrs.exe, um einen NULL-Session-Freigabeordner zu erstellen.

So konfigurieren Sie einen Netzwerkserver für die Softwareverteilung

1. Um einen freigegebenen Ordner auf dem Netzwerkserver einzurichten, klicken Sie mit der rechten Maustaste auf den Ordner, der freigegeben werden soll, und dann auf **Freigabe**.
2. Klicken Sie auf **Diesen Ordner freigeben** und anschließend auf **Berechtigungen**.
3. Fügen Sie die Gruppen **Jeder** und **Gast** hinzu; weisen Sie ihnen jedoch nur Leseberechtigungen zu. Fügen Sie in einer Domänenumgebung zusätzlich die Gruppe **Domänencomputer** hinzu und erteilen Sie ausschließlich Leseberechtigungen. Übernehmen Sie die Änderungen.
4. Konfigurieren Sie die Anmeldeinformationen für den bevorzugten Paketserver wie unter "Konfigurieren von bevorzugten Servern " auf Seite 913 beschrieben.
5. Kopieren Sie die Softwareverteilungspakete in diesen Ordner auf dem Netzwerkserver.

Sofern der Speicherplatz der Festplatte dies zulässt, können Sie Pakete in beliebiger Größe und Anzahl auf dem Netzwerkserver speichern.

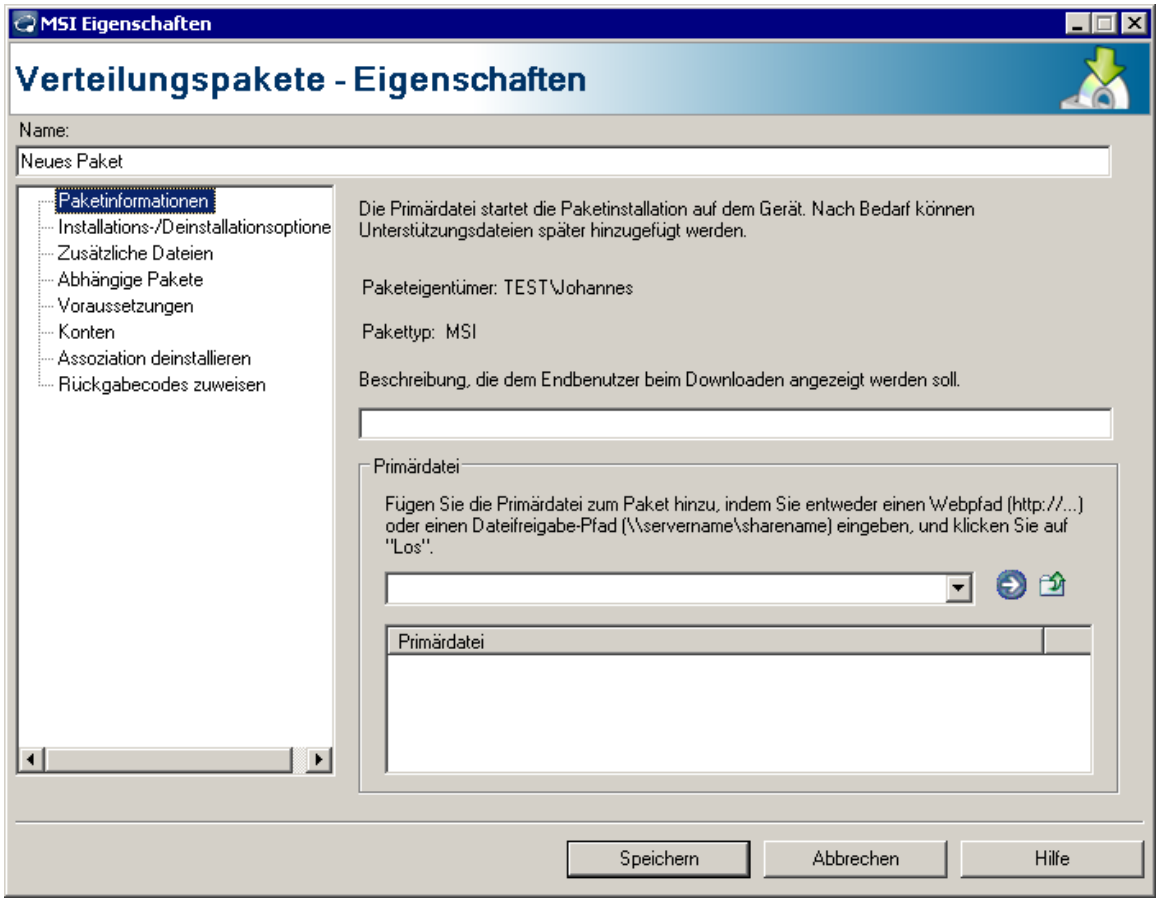
Verteilen eines Pakets

Ein Verteilungspaket besteht aus der Paketdatei, die Sie verteilen möchten, sowie aus zusätzlichen vom Paket benötigten Dateien und Einstellungen, die die Paketkomponenten und das Paketverhalten beschreiben. Damit Sie die Verteilungspaketdefinition für das Paket erstellen können, müssen Sie zuerst das Paket erstellen.

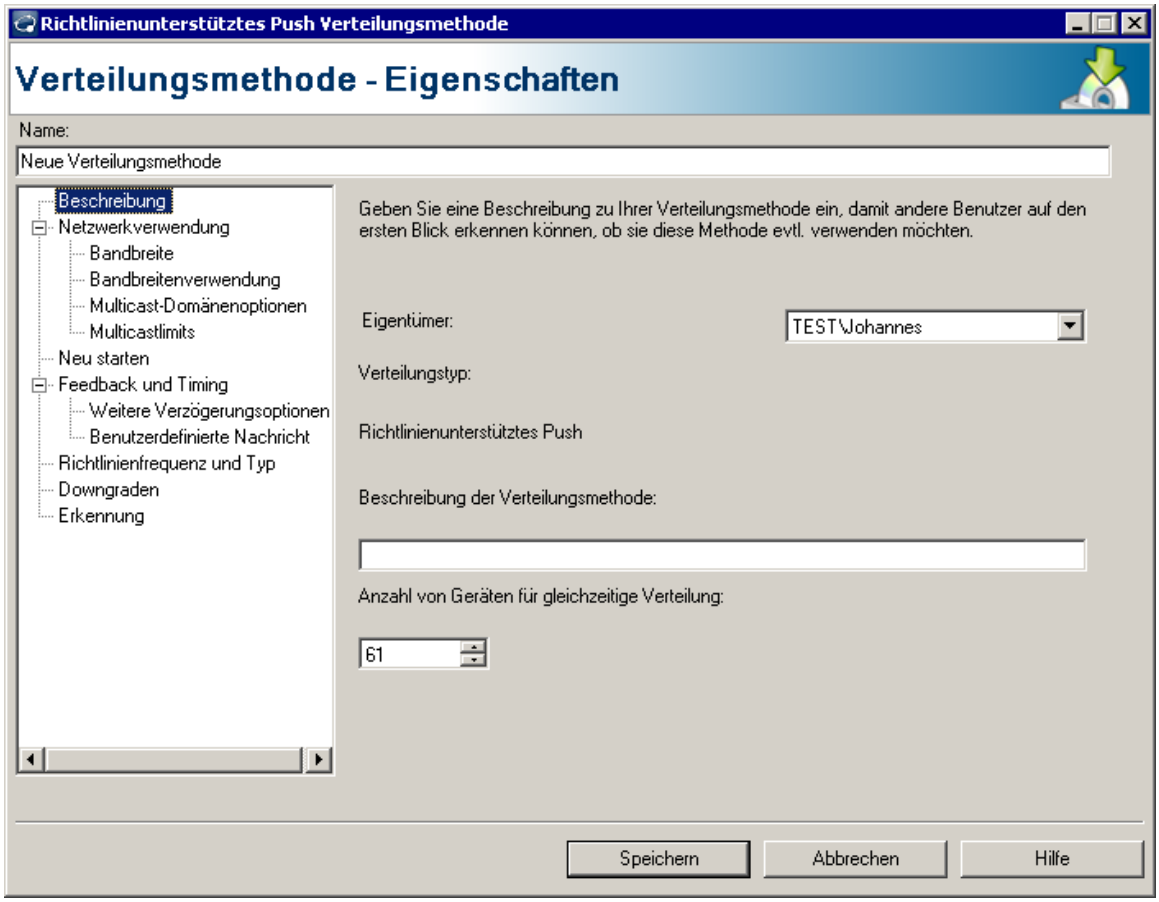
In diesen Anweisungen wird beschrieben, wie ein Softwareverteilungspaket erstellt wird. Damit das Paket richtig ausgeführt wird, muss das Softwareverteilungspaket auf einem Netzwerk- oder Webserver zur Verfügung stehen und auf den Geräten der Softwareverteilungsagent installiert sein.

Die Verteilung eines Pakets an die Geräte umfasst im Wesentlichen drei Schritte.

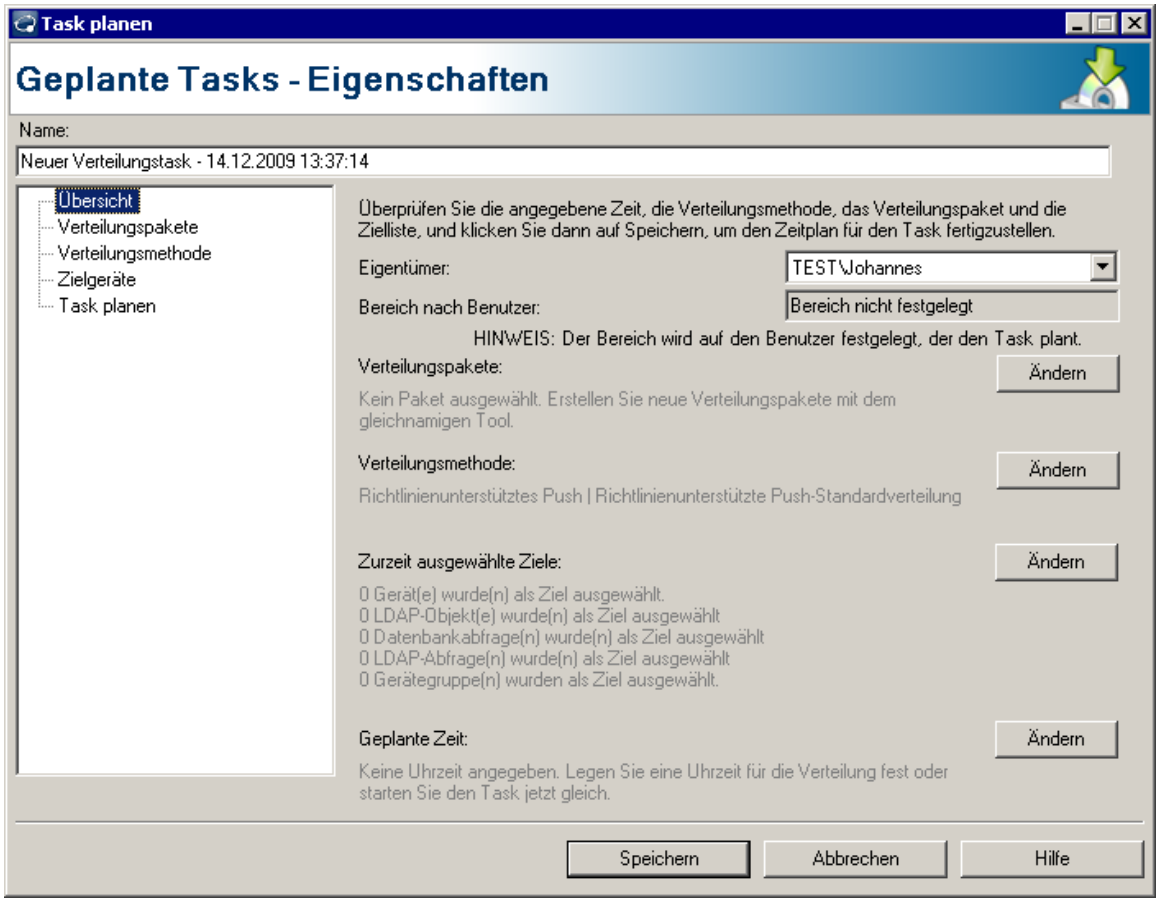
Schritt 1: Erstellen eines Verteilungspakets für das zu verteilende Paket.



Schritt 2: Auswählen der Verteilungsmethode.



Schritt 3: Planen des Pakets und der Verteilungsmethode für die Verteilung


Task planen
Geplante Tasks - Eigenschaften
Name:
Neuer Verteilungstask - 14.12.2009 13:37:14
Übersicht
Verteilungspakete
Verteilungsmethode
Zielgeräte
Task planen
Überprüfen Sie die angegebene Zeit, die Verteilungsmethode, das Verteilungspaket und die Zielliste, und klicken Sie dann auf Speichern, um den Zeitplan für den Task fertigzustellen.
Eigentümer:
TEST\Johannes
Bereich nach Benutzer:
Bereich nicht festgelegt
HINWEIS: Der Bereich wird auf den Benutzer festgelegt, der den Task plant.
Verteilungspakete:
Ändern
Kein Paket ausgewählt. Erstellen Sie neue Verteilungspakete mit dem gleichnamigen Tool.
Verteilungsmethode:
Ändern
Richtlinienunterstütztes Push | Richtlinienunterstützte Push-Standardverteilung
Zurzeit ausgewählte Ziele:
Ändern
0 Gerät(e) wurde(n) als Ziel ausgewählt.
0 LDAP-Objekt(e) wurde(n) als Ziel ausgewählt
0 Datenbankabfrage(n) wurde(n) als Ziel ausgewählt
0 LDAP-Abfrage(n) wurde(n) als Ziel ausgewählt
0 Gerätegruppe(n) wurden als Ziel ausgewählt.
Geplante Zeit:
Ändern
Keine Uhrzeit angegeben. Legen Sie eine Uhrzeit für die Verteilung fest oder starten Sie den Task jetzt gleich.
Speichern
Abbrechen
Hilfe

So erstellen Sie ein Verteilungspaket

1. Erstellen Sie das Paket, das Sie verteilen möchten.
2. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
3. Klicken Sie im Kontextmenü der gewünschten Paketgruppe auf **Neues Verteilungspaket** > Pakettyp, den Sie erstellen möchten.
4. Geben Sie im Dialogfeld **Verteilungspakete** die Paketinformationen ein und ändern Sie nach Bedarf die Optionen. Beachten Sie, dass Sie den Paketnamen, eine Beschreibung und Primärdatei eingeben müssen. Weitere Informationen zu den einzelnen Seiten finden Sie in der **Hilfe**.
5. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben. Ihr Skript wird unter dem Strukturelement für den von Ihnen ausgewählten Pakettyp und Eigentümer angezeigt.

HINWEIS: LANDesk stellt für jeden Verteilungsmethodentyp Standardkonfigurationen für Verteilungsmethoden bereit. Die in diesen Standardmethoden definierten Standardeinstellungen sollten in den meisten Umgebungen gut funktionieren. Wenn Sie eine dieser Standardmethoden ändern möchten, sollten Sie mit Kopieren und Einfügen ein Duplikat der Verteilungsmethode erstellen und dieses umbenennen, um die Standardwerte in der Originaldatei für den zukünftigen Gebrauch zu bewahren.

So erstellen Sie eine Verteilungsmethode (nur notwendig, wenn sich eine Standardverteilungsmethode für Ihre Umgebung nicht eignet)

1. Wenn Sie bereits eine Verteilungsmethode definiert haben, die Sie verwenden möchten (oder wenn Sie eine der Standardverteilungsmethoden verwenden), können Sie diesen Schritt überspringen und zum Abschnitt "So planen Sie einen Verteilungstask" wechseln.
2. Klicken Sie auf **Extras > Verteilung > Verteilungsmethoden**.
3. Klicken Sie mit der rechten Maustaste auf die Verteilungsmethode, die Sie verwenden möchten, und klicken Sie dann auf **Neue Verteilungsmethode**.
4. Geben Sie im Dialogfeld **Verteilungsmethode** die gewünschten Verteilungsdaten ein und ändern Sie nach Bedarf die Optionen. Weitere Informationen zu den einzelnen Seiten finden Sie in der **Hilfe**.
5. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben. Ihr Skript wird unter dem Strukturelement für die von Ihnen ausgewählte Verteilungsmethode und den von Ihnen ausgewählten Eigentümer angezeigt.

So planen Sie einen Verteilungstask

1. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Softwareverteilungstask erstellen**.
3. Wählen Sie auf der Seite **Verteilungspaket** das von Ihnen erstellte Verteilungspaket aus.
4. Wählen Sie auf der Seite **Verteilungsmethode** die gewünschte Verteilungsmethode aus.
5. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.
6. Ziehen Sie Ziele aus der Netzwerkansicht auf den Task im Fenster **Geplante Tasks**. Ziele können einzelne Geräte, Computergruppen LDAP-Objekte (Benutzer, Gerät und Gruppe), LDAP-Abfragen und Inventarabfragen beinhalten.
7. Klicken Sie im Kontextmenü des Tasks auf **Eigenschaften**.
8. Die Seite **Zielgeräte** zeigt, welche Geräte diesen Task erhalten.
9. Geben Sie auf der Seite **Task planen** den Namen und Zeitplan des Tasks ein.
10. Kehren Sie zur Seite **Übersicht** zurück und vergewissern Sie sich, dass der Task Ihren Vorstellungen entsprechend konfiguriert wurde.
11. Klicken Sie auf **Speichern**, wenn Sie den Vorgang abgeschlossen haben.

Verfolgen Sie den Taskverlauf im Fenster **Geplante Tasks**.

Verwenden von Verteilungseigentümern und Rechten

In Umgebungen mit mehreren Management Suite Benutzern lässt sich mitunter nicht immer einfach überblicken, für welche Verteilungspakete, Verteilungsmethoden und geplanten Tasks die einzelnen Benutzer verantwortlich sind. Um Sie bei diesem Problem zu unterstützen, macht Management Suite den Benutzer, der das Verteilungspaket, die Verteilungsmethode oder den geplanten Task erstellt hat, zum Standardeigentümer des betreffenden Objekts. Nur der Eigentümer und Benutzer der RBA Administrator-/Softwareverteilungskonfiguration können diese privaten Objekte anzeigen.

Private Objekte werden unter den Strukturen **Eigene Verteilungsmethoden**, **Eigene Pakete** oder **Eigene Tasks** angezeigt. Administrative Benutzer können für alle Benutzer Elemente unter den Strukturen **Alle Verteilungspakete**, **Alle Verteilungsmethoden** und **All Tasks** anzeigen.

Wenn Benutzer ein Verteilungsobjekt erstellen, verfügt die Seite **Beschreibung** über die Option **Eigentümer**. Benutzer können **Öffentlich** wählen, wenn das Objekt für alle Konsolenbenutzer sichtbar sein soll. Administratoren können zusätzlich zu **Öffentlich** einen bestimmten Benutzer auswählen.

Weitere Informationen zur Verwendung der rollenbasierten Administration in Verbindung mit der Softwareverteilung finden Sie unter "Softwareverteilung" auf Seite 56.

Verwenden mehrerer Verteilungspakete in einem Task

Pushbasierte, richtlinienbasierte und richtlinienunterstützte Push-Softwareverteilungstasks können ein Vorabpaket und ein endgültiges Paket umfassen. Bei Verwendung mehrerer Pakete werden die Pakete nacheinander installiert. Das vorherige Paket muss einen erfolgreichen Taskstatus auf allen Zielgeräten zurückgeben, bevor das nächste Paket installiert wird.

Vorabpakete und endgültige Pakete sind nützlich, wenn Sie vor und/oder nach dem Hauptpaket Befehle ausführen möchten. Beispiel: Sie können ein Batchdatei-Paket erstellen, das Befehle zum Konfigurieren des Zielgeräts für das Hauptpaket ausführt. Sie können festlegen, dass nach der Installation des Hauptpakets ein endgültiges Batchdatei-Paket ausgeführt wird, das alle erforderlichen Nachkonfigurationen ausführt. Jeder Pakettyp kann als Vorabpaket oder endgültiges Paket definiert werden, wobei als Verteilungsmethode jedoch immer "Push" gewählt werden muss. Die richtlinienbasierte Push-Verteilungsmethode unterstützt keine Vorabpakete oder endgültigen Pakete.

Sie können Vorabpakete und endgültige Pakete beim Planen eines Verteilungstasks spezifizieren. Die Seite **Verteilungspaket** des Dialogfelds **Geplanter Task - Eigenschaften** verfügt über die Optionen **Vorausgehendes Paket** und **Letztes Paket**. Bevor Sie auf eine dieser Optionen klicken können, müssen Sie zur Seite **Verteilungsmethode** wechseln und eine Push-Verteilungsmethode auswählen. Klicken Sie hierfür auf **Push** für den **Verteilungstyp** und klicken Sie dann auf die **Verteilungsmethode**, die Sie verwenden möchten.

So verwenden Sie mehrere Verteilungspakete in einem Task

1. Erstellen Sie die Pakete, die Sie in Ihrem Task verwenden möchten.
2. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**. Klicken Sie in der Symbolleiste auf die Schaltfläche **Softwareverteilung**.
3. Klicken Sie auf der Registerkarte **Verteilungsmethode** auf **Push** als **Verteilungstyp** und klicken Sie auf die **Verteilungsmethode**, die Sie verwenden möchten.
4. Klicken Sie auf der Registerkarte **Verteilungspaket** auf den **Pakettyp** und auf das **Verteilungspaket**, das Sie verwenden möchten.
5. Klicken Sie auf **Vorausgehendes Paket**, **Hauptpaket** oder **Letztes Paket**, je nachdem, welchen Pakettyp Sie installieren möchten, und klicken Sie auf **Festlegen**.
6. Wiederholen Sie die Schritte 4 und 5 für alle anderen Pakete, die Sie für diesen Task installieren möchten. Pro Stufe wird nur ein Paket unterstützt und es muss immer ein **Hauptpaket** vorhanden sein.
7. Schließen Sie die Taskkonfiguration ab und planen Sie den Task.

Informationen zu Dateidownloads

Die Softwareverteilung unterstützt mehrere Methoden, um die Datei zwecks Installation in das Gerät zu laden. Hierzu gehören:

- Abrufen der Datei aus dem Multicast-Cache
- Abrufen der Datei aus einem Peer

- Direkter Download von der Remotequelle

Wenn eine Datei heruntergeladen werden muss, überprüft SDClient (der Softwareverteilungsagent des Geräts) zuerst, ob sich die Datei im Cache befindet. Die Definition für den Cache ist entweder "C:\Programme\LANDesk\LDClient\sdmcache" oder der im "Cache Directory" unter dem Multicast-Registrierungsschlüssel gespeicherte Pfad:

- HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM\Distribution\Multicast

Die Struktur der Dateien im Cache ist mit der Struktur der Dateien auf dem Web- oder Netzwerkserver identisch. Dadurch können mehrere Pakete problemlos Dateien mit dem gleichen Namen haben.

Wenn sich die Datei nicht im Cache befindet, versucht der SDClient normalerweise, die Datei von einem Peer im Netzwerk downzuloaden. Sie können die Verteilungsmethode so konfigurieren, dass ein Peer-Download angefordert wird.

Wenn die Datei nicht von einem Peer abgerufen werden kann, lädt SDClient die Dateien direkt aus der UNC- oder URL-Quelle. Sie können die Verteilungsmethode so konfigurieren, dass beim Laden der Datei aus der Quelle nur ein Gerät in der Multicast-Domäne die Datei aus dem Speicherort der Quelle herunterladen wird. Beim Download von einer UNC-Freigabe wird in den meisten Fällen zur Bedingung gemacht, dass es sich bei der UNC-Freigabe um eine NULL-Session-Freigabe handelt. Wenn die Datei, die heruntergeladen werden muss, URL-basiert ist, lädt SDClient die Datei von der Website herunter.

In jedem Fall legt SDClient die Datei im Multicast-Cache ab. Sobald sich die Datei im Multicast-Cache befindet, verarbeitet SDClient die heruntergeladene Datei.

Eine in den Cache heruntergeladene Datei verbleibt mehrere Tage im Cache, jedoch wird sie irgendwann wieder aus dem Cache gelöscht. Die Zeitspanne, die die Datei im Cache gespeichert bleibt, wird von der bei der Paketbereitstellung verwendeten Verteilungsmethode gesteuert.

Aktualisieren von Pakethashes

Da viele Paketdateien von Peers im Netzwerk abgerufen werden, werden die Dateien vor dem Installieren überprüft. Die Integrität der Dateien wird durch den Vergleich des MD5-Hash der heruntergeladenen Datei mit dem auf dem Coreserver generierten MD5-Hash ermittelt.

Wenn ein Verteilungspaket erstmalig eingeplant wird, lädt Management Suite die Dateien herunter und berechnet die Hashwerte, die mit der Primärdatei sowie mit allen vom Verteilungspaket verwendeten Dateien verknüpft sind. Wenn das mit dem Paket gespeicherte Hash nicht mit dem Hashwert übereinstimmt, der von SDClient auf dem Zielgerät errechnet wurde, gilt der Download als ungültig.

Wenn Sie außerhalb von Management Suite Änderungen an dem betreffenden Paket vornehmen (wenn Sie z. B. den Paketinhalt aktualisieren), müssen Sie den Hash zurücksetzen, da andernfalls alle geplanten Tasks, an denen das aktualisierte Paket beteiligt ist, misslingen.

So setzen Sie ein Pakethash zurück

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Klicken Sie im Kontextmenü für das Paket, dessen Hash Sie aktualisieren möchten, auf **Dateihashes zurücksetzen**. Dieser Vorgang kann bei größeren Paketen mehrere Minuten in Anspruch nehmen.

Ausführen von Verteilungspaketen vom Quellserver

Die Softwareverteilung lädt normalerweise Paketdateien in den Cache des lokalen Geräts herunter und installiert das Paket vom Cache her. Dies führt u. U. zu keinem zufriedenstellenden Ergebnis, wenn ein Paket oder eine Anwendung Installationsdateien in einer bestimmten Ordnerstruktur sucht, wie z. B. dem Microsoft Office Installer, oder wenn die Anwendungsinstallation nicht alle Quelldateien für jede Installation verwendet.

In solchen Fällen können Sie stattdessen den lokalen Softwareverteilungsagenten dazu veranlassen, die Datei direkt von der Quelle aus auszuführen, ob dies nun ein bevorzugter Server ist oder die im Paket angegebene Quelle. Wenn Sie die Ausführung von der Quelle aktivieren, wird die Softwareverteilung keine Pakete in den lokalen Cache herunterladen und das Paket auch nicht von einem Peer her ausführen.

Wenn Sie die Ausführung von der Quelle mit in Webfreigaben gespeicherten Paketen wählen, muss die primäre Datei eine MSI-Datei oder ein SWD-Paket sein. Bei UNC-Freigaben kann die primäre Datei einem beliebigen Typ angehören.

So erstellen Sie eine Verteilungsmethode, die von der Quelle her ausgeführt wird

1. Klicken Sie auf **Extras > Verteilungsmethoden > Netzwerkverwendung**.
2. Klicken Sie auf **Dateien mit 'Ausführen aus Quelle' bereitstellen**.
3. Stellen Sie die Konfiguration der Verteilungsmethode fertig.

Verwenden der Softwareverteilung mit Paketen in einem verteilten Dateisystem (DFS)

Verteilte Dateisysteme (DFS, Distributed File System) verwenden mehrere Server zum Bereitstellen von Dateien, die von einer einzelnen Dateifreigabe her verfügbar sind. Die Standardmethode der Softwareverteilung zum Erkennen von Bandbreite in einem DFS-Szenario verwendet schließlich den Stammserver zum Berechnen der Bandbreite, der evtl. nicht der Server ist, der die Datei bereitstellt. Die Softwareverteilung stellt nun eine optionale Art zum Berechnen der Bandbreite bereit. Mit dieser neuen Methode wird bei der Bandbreitenerkennung auch ein kleiner Teil der Datei abgerufen, die tatsächlich verteilt wird. Auf diese Art berechnet die Softwareverteilung die Bandbreite vom Server, der die Datei bereitstellt.

Diese alternative Methode zur Bandbreitenerkennung ist standardmäßig nicht aktiviert. Sie können diese Option von der Datei "ntstacfg.in#-" im Ordner "ldlogon" des Coreservers her aktivieren. Wenn Sie diese Datei aktiviert haben, werden die Änderungen Teil von neuen oder aktualisierten Agentenkonfigurationen. Sie müssen Ihre Agentenkonfiguration erneut an Geräte verteilen, damit die Änderung in Kraft tritt.

Suchen Sie diesen Abschnitt in ntstacfg.in# und die nötigen Änderungen vornehmen.

```
; Die folgenden Registrierungswerte steuern die Bandbreitenerkennung nach Dateidownload
; ändern Sie den Wert UseDownloadForBandwidth in 1, um die Verwendung des Dateidownloads zur
Bandbreitenerkennung zu aktivieren
; der Wert DownloadSize sollte als Hex-Wert zwischen 400 und FFFF(1024 Byte bis 65535 Byte) eingegeben
werden.
REG1=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\UseDownloadForBandwidth, 0, , REG_DWORD
REG2=HKEY_LOCAL_MACHINE, SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DownloadSize,
2000, , REG_DWORD
```

Checkpunkt-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung

Management Suite 8 und neuere Versionen unterstützen bei der Verteilung Checkpunkt-Neustarts auf Byte-Ebene und dynamische Bandbreitendrosselung. Checkpoint-Neustarts werden von Verteilungsaufträgen unterstützt, die von SWD zuerst in den Cache-Ordner des Geräts (standardmäßig C:\Programme\LANDesk\LDClient\SDMCACHE) kopiert werden. Wenn eine Bandbreitensteuerungsoption ausgewählt wird, werden die Dateien zuerst in den Cache des Geräts kopiert; mithilfe von "Checkpoint-Neustart" können dann unterbrochene Verteilungsvorgänge an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden.

Dynamische Bandbreitendrosselung legt fest, dass der von einem Gerät erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Mit dieser Option wird zudem durchgesetzt, dass die gesamte Datei in den Cache des Geräts heruntergeladen wird. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byte-Ebene aktiviert. Das heißt, dass Downloadvorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden. Wenn Sie diese Option auswählen und die Prozentangabe für **Minimal verfügbare Bandbreite** auf 0 belassen, wird die Verteilung auf etwa ein Paket pro Sekunde gedrosselt, sobald das Gerät Netzwerkverkehr initiiert, und bleibt auf diesem Niveau, bis der Netzwerkverkehr endet. Wenn Sie den Wert für die minimal verfügbare Bandbreite heraufsetzen, reserviert das System ungefähr die von Ihnen angegebene Menge an Gerätebandbreite für die Verteilung, sofern die Verteilung Netzwerkbandbreite benötigt und Anwendungen auf dem Gerät um Bandbreite konkurrieren.

Wenn Sie ein SWD- oder MSI-Paket erneut installieren oder reparieren, sollten Sie die Option für die dynamische Bandbreitendrosselung nicht verwenden, weil bei diesen Pakettypen normalerweise nur die benötigten Dateien heruntergeladen werden. In diesem Fall würde durch den Einsatz der dynamischen Bandbreitendrosselung auch dann ein Download des gesamten Pakets erzwungen, wenn nur ein kleiner Teil des Pakets zur Reparatur benötigt wird.

Sie können "kollektive Bandbreitendrosselung" konfigurieren, sodass nur ein Gerät aus der Multicast-Domäne Dateien aus der Remotequelle herunterladen wird. Sie können auch die beim Download von der Quelle verwendete Bandbreitenmenge konfigurieren. Diese Funktion ist auf allen Versionen des Windows-Systems verfügbar. Kollektive Bandbreitendrosselung wird auf Macintosh-Systemen nicht unterstützt.

Softwareverteilung mit Targeted Multicast

Mit der LANDesk Targeted Multicast-Technologie können Sie große Pakete als Massen-Rollout im Netzwerk verteilen und dabei die Netzwerkbelastung so gering wie möglich halten. Die Targeted Multicast-Funktionen benötigen zur Unterstützung von Multicast-Paketen weder eine zusätzliche Hardware- oder Softwareinfrastruktur noch spezielle Routerkonfigurationen. Sie profitieren von den enormen Vorteilen der Multicast-Technologie ohne die sonst üblichen Probleme.

Targeted Multicast unterstützt Ihre vorhandenen Softwareverteilungspakete. Mit Targeted Multicast lassen sich Softwarepakete ganz einfach verteilen, selbst in WAN-Umgebungen mit mehreren Hops und niedriger Verbindungsgeschwindigkeit (56 KBit/s). Targeted Multicast verwendet HTTP für die Übermittlung von einer Website an einen Subnetzrepräsentanten. Der Management Suite Inventarscanner stellt dem Targeted Multicast-Dienst alle Subnetzinformationen zur Verfügung.

Targeted Multicast bietet zahlreiche Vorteile, die Standard-"Multicast"-Methoden nicht aufweisen. Mithilfe des inventarbasierten Targeting von Geräten können Sie ein Paket über ein Multicast an eine ausgewählte Gruppe von Computern senden, die bestimmte Kriterien erfüllen. Targeted Multicast ist auch deshalb unkompliziert, weil Router nicht extra für die Verarbeitung von übermittelten Paketen konfiguriert werden müssen.

Verglichen mit konventionellen Softwareverteilungsmethoden wird bei der Übermittlung von Softwarepaketen mit Targeted Multicast deutlich weniger Zeit und Bandbreite benötigt. Statt für jedes Gerät ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt. Je höher die Anzahl der Gerät im jeweiligen Subnetz, umso mehr Bandbreite wird eingespart.

Sie können Targeted Multicast von den Eigenschaften der Verteilungsmethode aus aktivieren, indem Sie die Option **Dateien mit Multicast bereitstellen** in den Eigenschaften für **Verteilungsmethoden** auf der Seite **Netzwerkverwendung** auswählen. Multicast wird in richtlinienbasierten Push- sowie Push- und Multicast-Verteilungsmethoden (nur Cache) unterstützt. Unter der Seite **Netzwerkverwendung** befinden sich mehrere Seiten, mit denen der Multicast-Vorgang konfiguriert werden kann.

Wenn Sie eine Verteilung mithilfe von Targeted Multicast starten, wird das Fenster **Multicast Software Distribution** angezeigt. Dieses Fenster enthält ausführliche Informationen zum Verteilungsvorgang. Weitere Informationen zur Bedeutung der einzelnen Felder erhalten Sie, wenn Sie im Fenster **Multicast Software Distribution** auf die Schaltfläche **Hilfe** klicken.

Sowohl Windows- als auch Macintosh OS 10.2-Geräte unterstützen Targeted Multicast. Darüber hinaus können Sie Betriebssystem-Bereitstellungsabbilder per Multicast übermitteln.

Verwenden von Peerdownload

Peerdownload ist eine Targeted Multicast-Option, die Zielgeräte zwingt, ein Paket aus dem lokalen Cache des Geräts oder von einem Peer im gleichen Subnetz zu installieren. Diese Option reduziert zwar den Netzwerkverkehr, die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer befindet.

Auch wenn Sie die Option **Peerdownload** nicht auswählen, versucht der Targeted Multicast-Geräteagent, Bandbreite zu sparen, indem er die folgenden Speicherorte in der unten angegebenen Reihenfolge nach Paketdateien überprüft:

1. Lokaler Cache
2. Peer im gleichen Subnetz
3. Paketserver

Kopieren von Dateien in den Multicast-Ordner im lokalen Cache

Sie können eine oder mehrere Dateien mithilfe von Multicast in den Multicast-Ordner im lokalen Cache kopieren. Mit dieser Option wird eine Datei in den lokalen Cache der Zielgeräte kopiert. Die Datei wird damit nicht installiert oder in irgendeiner anderen Weise verarbeitet. Diese Option ist hilfreich, um Dateien auf Multicast-Domänenrepräsentanten oder einem Gerät in jeder der Multicast-Domänen bereitzustellen. Sie können eine erstmalige Bereitstellung auf Domänenrepräsentanten ausführen und dann die Bereitstellung mit der Option "Peerdownload" wiederholen. Auf diese Weise vergewissern Sie sich, dass die Geräte die Pakete nur von einem Peer in deren Subnetz herunterladen.

Konfigurieren von Targeted Multicast

Bevor Sie Targeted Multicast verwenden können, müssen Sie sicherstellen, dass sich die Targeted Multicast-Komponenten in dem Subnetz befinden, an das die Pakete verteilt werden sollen. Targeted Multicast erfordert Management Suite Agenten und einen Multicast-Domänenrepräsentanten.

So geben Sie manuell an, welche Computer als Multicast-Domänenrepräsentanten verwendet werden sollen

1. Klicken Sie in der Netzwerkansicht auf **Konfiguration > Multicast-Domänenrepräsentanten**.
2. Fügen Sie Domänenrepräsentanten hinzu, indem Sie die Computer, die als Repräsentanten fungieren sollen, von der Netzwerkansicht in diese Kategorie ziehen.

Targeted Multicast verwendet den ersten Computer in der Gruppe **Multicast-Domänenrepräsentanten**, der pro Subnetz reagiert.

Nur Windows-Computer können als Multicast-Domänenrepräsentanten fungieren. Wenn Sie Pakete über Targeted Multicast an Macintosh-Computer verteilen möchten, müssen Sie sicherstellen, dass zur Multicast-Domäne mindestens ein Windows-Computer gehört, der für die Macintosh-Computer als Domänenrepräsentant dienen kann. Wenn es in einer vorwiegend mit Macintosh-Computern bestückten Umgebung nur wenige Windows-Computer gibt, sollten Sie die Windows-Domänenrepräsentanten in der Gruppe "Multicast-Domänenrepräsentanten" manuell festlegen.

Sie können Multicasts drosseln, indem Sie die Einstellung der Schieberegler für die Bandbreite auf der Seite **Bandbreitenverwendung** unter der Seite **Netzwerkverwendung** in den Verteilungsmethodenfenstern **Richtlinienunterstütztes Push**, **Push** und **Multicast** ändern.

Sie können die Targeted Multicast-Optionen im Dialogfeld "Management Suite Dienste konfigurieren" auch anpassen. Um den Targeted Multicast-Dienst zu konfigurieren, klicken Sie auf die Registerkarte **Konfigurieren > Dienste > Multicast**. Klicken Sie in der Registerkarte auf **Hilfe**, um weitere Informationen zu erhalten.

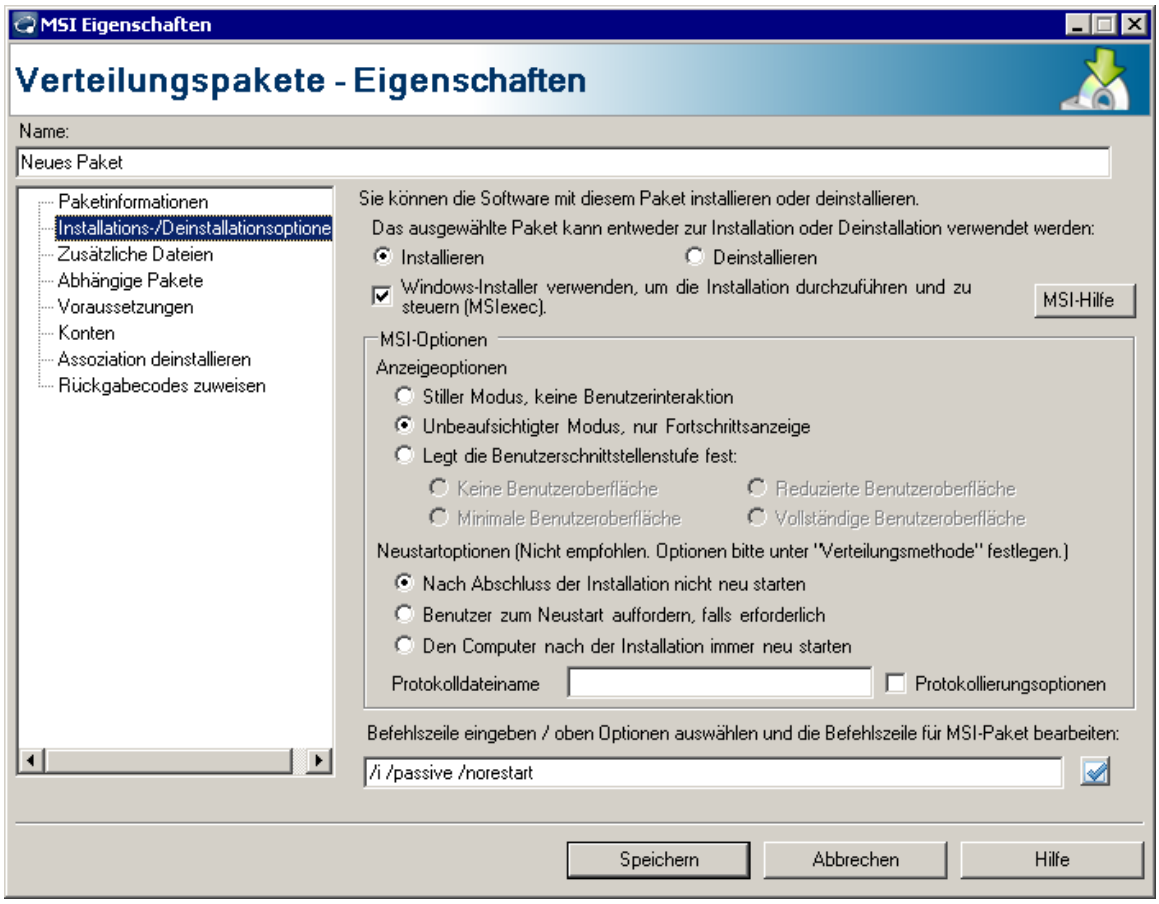
Verwenden von MSI-Verteilungspaketen

Management Suite unterstützt die MSI-Installation mit vollständiger Statusberichterstattung und MSI-Paketerkennung. Der Typ des MSI-Verteilungspakets ist die von Management Suite bevorzugte Methode der Softwareverteilung. Eine fundierte Kenntnis der MSI-Parameter ist beim Setup der MSI-Pakete und Verteilungsmethoden von Vorteil.

Verwenden von MSI-Befehlszeilenparametern mit der Softwareverteilung

Wenn Sie ein MSI-Verteilungspaket installieren, setzt Management Suite die MSI API-Aufrufe ein. MSI-Installationen verwenden zwei verschiedene Typen von Befehlszeilenparametern:

- Optionsparameter
- Eigenschaftsreferenzparameter



Optionsparameter

Optionsparameter sind Switches, die vom Microsoft-Installationstool Msiexec.exe verwendet werden. Beispielsweise ist der /q-Switch ein häufig eingesetzter Switch für Msiexec, der die unbeaufsichtigte Installation im Hintergrund ausführt.

Im Dialogfeld **Verteilungspakete - Eigenschaften** können Sie MSI-Optionsparameter auf der Seite **Installations-/Deinstallationsoptionen** im Feld **Befehlszeile** eingeben. Klicken Sie auf die Schaltfläche mit dem Häkchen neben dem Feld, um die Befehlszeile zu validieren. Weitere Informationen über die Msiexec-Optionen finden Sie hier: http://support.microsoft.com/?kbid=227091.

Eigenschaftsreferenzparameter

Eigenschaftsreferenzen, auch öffentliche Eigenschaften genannt, gelten speziell für die MSI-Datei. Die Parameter werden direkt an die MSI-Installations APIs weitergegeben. Sie können im Feld **Befehlszeile** der **Installations-/Deinstallationsoptionen** eines MSI-Verteilungspakets verwendet werden.

Die Syntax der Eigenschaftsreferenzen lautet PROPERTY=VALUE. Eine allgemeine Eigenschaftsreferenz ist die Transformationseigenschaft. Diese Eigenschaft ruft eine .mst-Datei (Transformation) auf. Weitere Informationen über die Eigenschaftsreferenzparameter finden Sie hier: http://support.microsoft.com/?kbid=230781.

Informationen über öffentliche Eigenschaften einer Anwendung finden Sie in der Dokumentation zur Softwareinstallation, der offiziellen Webseite der Anwendung oder direkt beim Softwareanbieter.

Ausführen einer MSI im Hintergrund

In Management Suite wird die im Hintergrund ablaufende MSI automatisch unter **Installations-/Deinstallationsoptionen** einer Verteilungsmethode behandelt. Um eine MSI im Hintergrund auszuführen, gehen Sie zur Seite **Installations-/Deinstallationsoptionen** der gewünschten Verteilungsmethode und klicken auf **Stiller Modus, keine Benutzerinteraktion**.

Automatisierung einer MSI-Installation

Für viele MSIs gilt, dass die Ausführung im Hintergrund die MSI auch automatisiert. In diesen Fällen müssen Sie für die Automatisierung einer MSI-Installation nur **Stiller Modus, keine Benutzerinteraktion** in der Verteilungsmethode auswählen.

Manchmal ist eine Eigenschaftsreferenz nötig, damit die Installation ausgeführt werden kann. Dann fordert das MSI-Installationsprogramm zur Eingabe eines Wertes auf. Bei der automatischen Installation kommt diese Aufforderung nicht vor. Die MSI-Installation schlägt fehl und bringt die MSI Standardfehlermeldung 1603 hoch: Schwerwiegender Fehler bei der Installation. Die erforderlichen öffentlichen Eigenschaften sollten einem Wert im Feld **Befehlszeile** des Verteilungspakets zugewiesen werden.

Verwenden einer Transformationsdatei bei einer MSI-Installation

Antwortdateien für MSIs heißen Transformationsdateien und enden in einer .mst-Erweiterung. Nicht alle MSI-Installationen benötigen eine Transformationsdatei. Sie kann jedoch verwendet werden, wenn es zu viele Eigenschaftsreferenzen gibt, deren Werte geändert oder zugewiesen werden müssen. Wenn es von der Anwendung unterstützt wird, kann eine Antwortdatei erstellt werden, die an alle Eigenschaftsreferenzparameter weitergeleitet wird.

Ist eine Transformationsdatei erforderlich, die jedoch nicht bei der Installation bereitgestellt wird, dann tritt der Fehler 1603 auf: Schwerwiegender Fehler bei der Installation. Der Softwarevertreiber hat oftmals die nötigen Informationen oder ein Tool, um eine Transformationsdatei für sein spezielles MSI zu erstellen. Beispielsweise sollte für die Bereitstellung der Volumenlizenzversion von Microsoft Office 2003 eine Transformationsdatei verwendet werden. Microsoft hat ein Tool namens "Custom Installation Wizard", das als Teil des Office 2003 Ressourcenkits installiert wird. Das Office 2003 Ressourcenkit kann über die folgende Webseite heruntergeladen werden:

- http://download.microsoft.com/download/0/e/d/0eda9ae6-f5c9-44be-98c7¬ccc3016a296a/ork.exe

Wenn der Vertreiber nicht über die nötige Information oder ein solches Tool verfügt, bietet Microsoft das sogenannte Orca-Tool an, das eine Transformationsdatei erstellen kann. Weitere Unterstützung finden Sie in der Orca-Hilfedatei.

Neustarts mit einer MSI-Installation handhaben

Management Suite handhabt MSI-Neustarts über die Seite **Neustart** in den Eigenschaften der Verteilungsmethoden. LANDesk gibt automatisch die Parameter REBOOT=REALLYSUPPRESS und /NORESTART weiter, wenn Sie in der Verteilungsmethode **Nie neu starten** auswählen.

Die Option **Immer neu starten** gibt den Parameter /FORCESTART weiter.

Nur bei Bedarf neu starten gestattet dem MSI, den Neustart zu handhaben. Ist Feedback aktiviert, dann kann der Benutzer aufgefordert werden, einen Neustart durchzuführen. Es ist wichtig, zu wissen, dass MSIs benutzerdefinierte Aktionen unterstützt. Wenn eine benutzerdefinierte Aktion einen Neustart einleitet, kann Management Suite nichts dagegen tun.

MSI Checkliste

Wenn eine Bereitstellung ein MSI beinhaltet, gehen Sie gemäß dieser Checkliste vor.

- Ich habe die richtige Version der Installationsdateien, einschließlich das MSI und alle zusätzlichen Dateien, für eine Volumenlizenzbereitstellung.
- Ich habe die Informationen vom Softwarevertreiber, wie man die Softwareinstallation und -konfiguration automatisiert und im Hintergrund ausführt, sowie zur Handhabung von Neustarts.
- Ich weiß, welche öffentlichen Eigenschaftsparameter ich an das MSI weitergeben muss.
- Ich weiß, ob dieses MSI eine Transformationsdatei zur Installation benötigt und habe für diesen Fall eine solche erstellt.

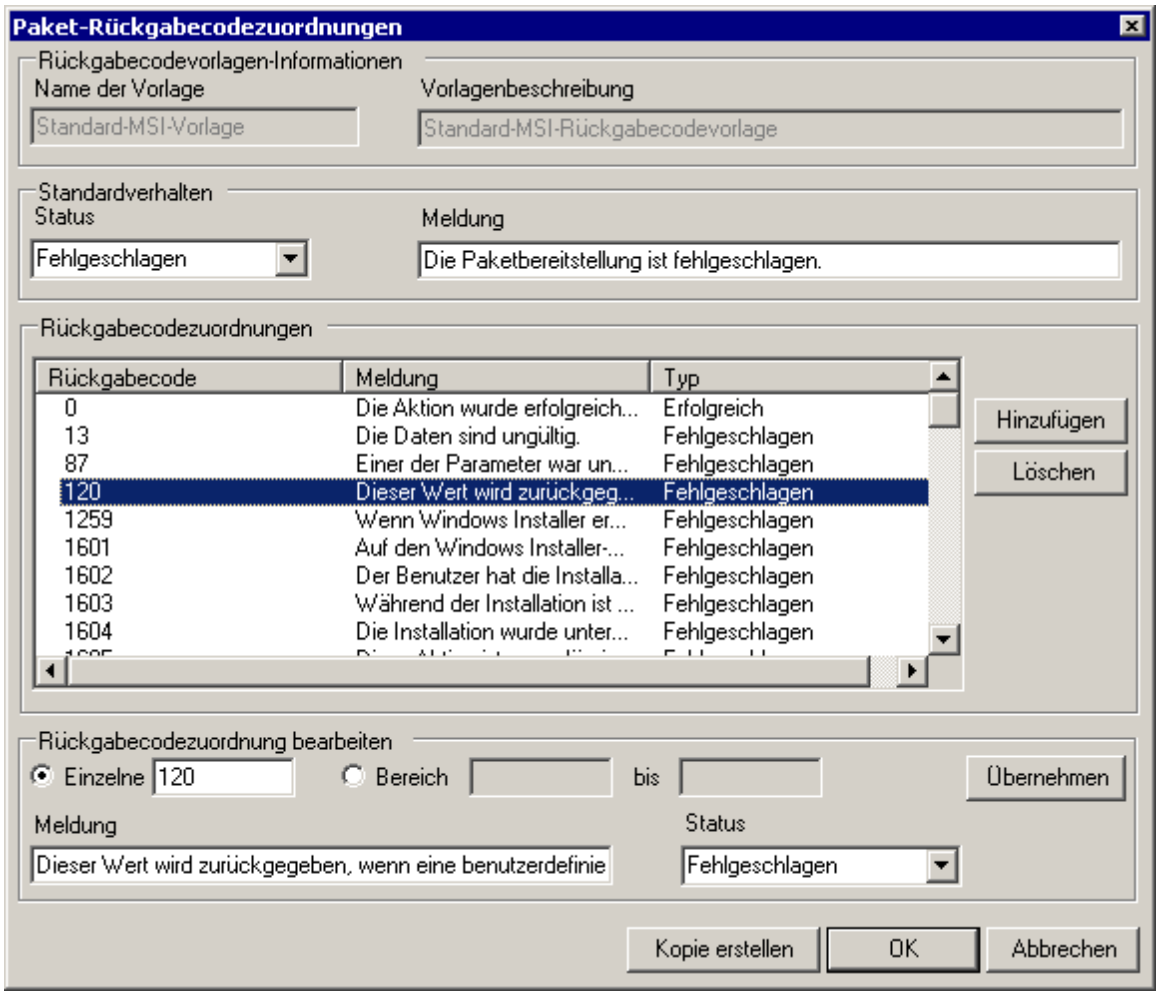
Zuweisen von Rückgabecodes für die Verteilung

Das Dialogfeld "Rückgabecodes zuweisen" wird dazu verwendet, den Status an den Coreserver zurückzumelden und dabei anzuzeigen, ob der Verteilungstask erfolgreich ausgeführt wurde oder nicht. In der Vergangenheit wurde in der Management Suite nur "0" als Erfolg interpretiert und jede andere Rückmeldung als Fehler oder Misserfolg. Hieraus ergab sich für Administratoren das Problem, dass Management Suite einen Misserfolg gemeldet hat, obwohl die Anwendung unter Umständen fehlerfrei installiert wurde, der Rückgabecode jedoch in Form einer anderen Zahl als Null (0) erfolgte.

Anbieter verwalten von Produktentwicklern erstellte Listen aller möglichen Rückgabecodes und den spezifischen Ergebnissen, die diese Codes anzeigen. Management Suite bietet Administratoren jetzt die Möglichkeit, in Rückgabecodelisten nachzuschlagen und Vorlagen zu erstellen, die mit einem Einzelpaket oder mit mehreren Paketen verknüpft werden können. Für jede Rückgabecode kann ein Administrator bestimmen, ob er Erfolg oder Misserfolg anzeigt und eine benutzerdefinierte Meldung zurücksenden, die die spezifischen Ergebnisse der Installation anzeigt. Management Suite wird jetzt mit einem Windows-Installationsprozess für Office 2003- und Office XP-Vorlagen geliefert. Weitere Informationen zu den in dieser Vorlage enthaltenen Rückgabecodes finden Sie hier: http://support.microsoft.com/kb/290158.

Abgesehen davon, dass Sie diese Funktion in Verbindung mit Anwendungen von Drittanbietern einsetzen können, haben Sie ferner die Möglichkeit, Rückgabecodevorlagen für proprietäre, betriebseigene Anwendungen zu erstellen, die von Entwicklern im eigenen Haus geschrieben wurden. Management Suite bietet neben einer Standardvorlage auch die Möglichkeit, neue benutzerdefinierte Vorlagen zu erstellen, die Standardvorlagen oder benutzerdefinierten Vorlagen zu kopieren oder mit der Rückgabecode-Vorlagenverwaltung Änderungen an beliebigen Vorlagen vorzunehmen. Bei der Vorlagenerstellung kann eine bestimmte Vorlage mit einem bestimmten Paket im Dialogfeld "Rückgabecodes zuweisen" über das Fenster "Paket-Rückgabecodezuordnungen" verknüpft werden. Von dort aus können auch Änderungen an Vorlagen vorgenommen werden.

Benutzer können wählen, ob sie alle möglichen Rückgabecodes hinzufügen wollen, die Erfolg oder Misserfolg anzeigen, oder nur zusätzliche Rückgabecodes zur Anzeige eines Erfolgs. Für den Fall, dass nur Erfolgscodes hinzugefügt werden, werden sämtliche Rückgabecodes, auf die in der Vorlage kein Bezug vorhanden ist, automatisch der Kategorie "Misserfolg" zugeordnet.



Management Suite enthält zwei Standardvorlagen:

- **Standard-MSI-Vorlage:** Enthält über 50 Zuordnungen, die die standardmäßigen MSI-Rückgabecodes abdecken.
- **Standard-Nicht-MSI-Vorlage:** Enthält eine einzige Zuordnung für den Rückgabecode 0: "Die Aktion wurde erfolgreich abgeschlossen." Alle Fehlercodes, die nicht 0 sind, geben die Meldung "Die Paketbereitstellung ist fehlgeschlagen." zurück.

Eine dieser Vorlagen wird dem Verteilungspaket in Abhängigkeit vom Pakettyp automatisch zugewiesen. Sie können die Vorlagenzuordnung in den Eigenschaften eines Verteilungspakets ändern.

Zuweisen von Rückgabecodes für die Verteilung

Das Dialogfeld "Rückgabecodes zuweisen" wird dazu verwendet, den Status an den Coreserver zurückzumelden und dabei anzuzeigen, ob der Verteilungstask erfolgreich ausgeführt wurde oder nicht.

Benutzer können wählen, ob sie alle möglichen Rückgabecodes hinzufügen wollen, die Erfolg oder Misserfolg anzeigen, oder nur zusätzliche Rückgabecodes zur Anzeige eines Erfolgs. Für den Fall, dass nur Erfolgscodes hinzugefügt werden, werden sämtliche Rückgabecodes, auf die in der Vorlage kein Bezug vorhanden ist, automatisch der Kategorie "Misserfolg" zugeordnet.

So verwenden Sie die Rückgabecode-Vorlagenverwaltung

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Klicken Sie in der Symbolleiste **Verteilungspakete** auf die Schaltfläche **Rückgabecode-Vorlagenverwaltung**.
3. Klicken Sie im Dialogfeld **Rückgabecode-Vorlagenverwaltung** auf **Hinzufügen, Ändern, Löschen, Importieren** oder **Exportieren**.
4. Klicken Sie auf **Speichern**.

So fügen Sie eine neue Rückgabecode-Zuordnungsvorlage hinzu

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Klicken Sie in der Symbolleiste **Verteilungspakete** auf die Schaltfläche **Rückgabecode-Vorlagenverwaltung**.
3. Klicken Sie im Dialogfeld **Rückgabecode-Vorlagenverwaltung** auf **Hinzufügen**.
4. Geben Sie einen **Vorlagennamen** und eine **Vorlagenbeschreibung** ein.
5. Wählen Sie einen **Vorlagenfiltertyp** aus.
6. Klicken Sie auf **OK**.
7. Wenn Sie die Standardmeldung für Erfolg oder Misserfolg ändern möchten, wählen Sie im Dialogfeld **Paket-Rückgabecodezuordnungen** einen **Status** und eine entsprechende **Meldung** für diesen Status aus.
8. Fügen Sie eine neue Zuordnung hinzu, indem Sie auf **Hinzufügen** klicken.
9. Geben Sie unten im Dialogfeld den numerischen Rückgabecode oder den Rückgabecodebereich ein.
10. Geben Sie eine **Meldung** ein und wählen Sie einen **Status** aus.
11. Wiederholen Sie die Schritte 8 bis 10 je nach Bedarf.
12. Klicken Sie auf **OK**. Ihre neue Vorlage erscheint in der Liste.

So übernehmen Sie die Rückgabecodezuordnung für ein Verteilungspaket

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Doppelklicken Sie auf das Paket, das Sie ändern möchten.
3. Klicken Sie im Baum "Paketeigenschaften" auf **Rückgabecodes zuweisen**.
4. Klicken Sie auf die Rückgabecodevorlage, die Sie anwenden möchten.
5. Klicken Sie auf **Zuweisen**.
6. Klicken Sie auf **Speichern**.

Exportieren und Importieren von Rückgabecodevorlagen für die Verteilung

Rückgabecodevorlagen werden in der Coredatenbank gespeichert, aber Sie können Vorlagen in eine XML-Datei exportieren und dann auf anderen Servern importieren. Wenn ein Verteilungspaket durch Coresynchronisierung synchronisiert wird, ist die ihm zugewiesene Rückgabecodevorlage Teil der Synchronisierungsdaten.

So exportieren Sie eine Rückgabecodevorlage

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Klicken Sie in der Symbolleiste **Verteilungspakete** auf die Schaltfläche **Rückgabecode-Vorlagenverwaltung**.
3. Klicken Sie auf die Vorlage, die Sie exportieren möchten.
4. Klicken Sie auf **Exportieren**.
5. Steuern Sie mit Durchsuchen einen Pfad an und geben Sie einen **Dateinamen** an.
6. Klicken Sie auf **Speichern**.

So importieren Sie eine Rückgabecodevorlage

1. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
2. Klicken Sie in der Symbolleiste **Verteilungspakete** auf die Schaltfläche **Rückgabecode-Vorlagenverwaltung**.
3. Klicken Sie auf **Importieren**.
4. Steuern Sie mit Durchsuchen die XML-Datei an, die eine exportierte Vorlage enthält.
5. Klicken Sie auf **Öffnen**.

Verwenden des Softwarebereitstellungsportals

Bei verwalteten Geräten erfolgt der Zugriff auf das Fenster des Softwarebereitstellungsportals über den Desktop Manager. Im Portalfenster sind alle Softwareverteilungspakettasks aufgeführt, die unter Verwendung einer richtlinienbasierten Verteilungsmethode verteilt wurden.

Wenn Sie das Portal starten, werden Sie aufgefordert, zu warten, während die Synchronisierung mit dem Richtlinienserver zur Aktualisierung der Anwendungsliste erfolgt. Während dieser Zeit erfolgt die Richtliniensynchronisierung und der Download eventuell vorhandener neuer Richtlinien. Die erforderlichen Richtlinien werden nicht im Fenster des Softwarebereitstellungsportals angezeigt und ihre Installation wird automatisch gestartet (es sei denn, der Endbenutzer verzögert dies). Die anderen Tasks werden im Fenster des Softwarebereitstellungsportals angezeigt.

Das verwaltete Gerät besitzt einen Richtlinien-Invokerdienst, der die heruntergeladenen Richtlinien untersucht. Die Richtlinientasks werden nach dem Abrufen in einer kleinen Datenbank gespeichert. Der Invokerdienst überwacht diese Datenbank und aktualisiert den Status der Richtlinien, wenn sie sich von einem Status zu einem anderen bewegen. Er liest außerdem dem Status von Richtlinien ein, um zu bestimmen, ob eine Installation stattfinden muss. Der Invoker installiert keine Pakete. Vielmehr ruft er den Softwareverteilungsagenten (sdclient.exe) auf und dieser führt dann die Installation durch.

Abgesehen vom Richtlinienupdate, das erfolgt, wenn ein Benutzer das Softwarebereitstellungsportal öffnet, wirken sich diese Agentenkonfigurationsoptionen auch auf die Richtlinienupdate-Intervalle aus: Ein Update erfolgt:

- bei der Anmeldung, wenn die Option **Wenn sich der Benutzer anmeldet** ausgewählt wurde,
- bei einer Änderung der IP-Adresse eines Benutzers, wenn die Option **Wenn sich die IP-Adresse ändert** ausgewählt wurde,
- im Local-Scheduler-Intervall, das Sie angeben, wenn Sie auf die Schaltfläche **Einstellungen ändern** klicken. In der Grundeinstellung verwenden verwaltete Geräte den Local-Scheduler, um einmal täglich Richtlinienupdates abzurufen.

Sie können diese Richtlinienupdate-Einstellungen im Dialogfeld der Agentenkonfiguration auf der Seite **Softwareverteilung > Richtlinienoptionen** ändern.

Verteilen von Softwareprodukten an Linux-Geräte

Sobald Sie die Linux-Agenten bereitgestellt haben, können Sie Softwareprodukte an Ihre Linux-Geräte verteilen. Die erstmalige Bereitstellung eines Linux-Agenten erfolgt über eine SSH-Verbindung. Nachdem die Agenten installiert sind, verwendet der Coreserver den Standard LANDesk Agenten, um mit dem Linux-Server zu kommunizieren und Dateien zu übertragen. Für die Verteilung von Software an ein Linux-Gerät benötigen Sie Administratorrechte

Sie können nur RPMs an Linux-Geräte verteilen. Die Linux-Agenten installieren automatisch jeden von Ihnen verteilten RPM. Der eigentliche RPM wird nach der Installation nicht auf dem Server gespeichert. Sie können den von Ihnen angegebenen RPM mithilfe der Softwareverteilung installieren und deinstallieren. Für die Linux-Softwareverteilung werden nur pushbasierte-Verteilungsmethoden unterstützt. Die Einstellungen in der pushbasierten Verteilungsmethode werden für die Linux-Softwareverteilung ignoriert, sodass es keine Rolle spielt, welche Pushverteilungsmethode Sie auswählen oder wie die Einstellungen darin lauten.

Die Verteilung läuft wie folgt ab:

1. Der Coreserver stellt über den Standard LANDesk Agenten eine Verbindung mit dem Linux-Gerät her.
2. Das Gerät lädt das Paket herunter.
3. Das Gerät führt ein Shell-Skript aus, das mithilfe von RPM-Befehlen das RPM-Paket installiert.
4. Das Gerät sendet den Status zurück an den Coreserver.

Sie können Linux-RPMs auf HTTP-Freigaben speichern. Die Linux-Softwareverteilung unterstützt keine UNC-Dateifreigaben. Stellen Sie im Falle von HTTP-Freigaben sicher, dass Sie für die betreffende Freigabe Directory-Browsing aktiviert haben. Wenn Sie eine HTTP-Freigabe auf einem Windows-Gerät verwenden, bei dem es sich nicht um den Core handelt, müssen Sie IIS mit dem korrekten MIME-Typ für RPM-Dateien konfigurieren. Andernfalls verhindert der von IIS verwendete Standard-MIME-Typ, dass RPM die Datei herunterladen kann.

So konfigurieren Sie den RPM MIME-Typ auf Windows-Geräten

1. Öffnen Sie unter Windows in der **Systemsteuerung** den **Internet Services Manager**.
2. Navigieren Sie zu dem Ordner, der als Host für Ihre Verteilungsdateien dient. Klicken Sie im Kontextmenü dieses Ordners auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **HTTP-Header** auf die Schaltfläche **Dateitypen**.
4. Klicken Sie auf **Neuer Typ**.
5. Geben Sie als **Verknüpfte Erweiterungrpm** ein. Beachten Sie, dass rpm in Kleinbuchstaben einzugeben ist.
6. Geben Sie als **Inhaltstyp** text/plain ein.
7. Klicken Sie auf **OK**, um das Dialogfeld zu schließen.

Sobald Sie die Dateien auf Ihrer Paketfreigabe gespeichert haben, erstellen Sie ein neues Linux-Verteilungspaket im Fenster **Verteilungspakete**, verknüpfen es mit der gewünschten Verteilungsmethode und planen die Verteilung.

Erläuterungen zu den Linux-Software-Abhängigkeiten

Wenn Sie auf **Speichern** im Dialogfeld **Verteilungspakete - Eigenschaften** eines Linux-Pakets klicken, analysiert die Softwareverteilung den primären RPM und alle von Ihnen ausgewählten abhängigen RPMs auf Abhängigkeiten, die die RPMs erfordern. Diese Abhängigkeiten werden dann im Dialogfeld **Fehlende Bibliotheken** angezeigt. Wenn Sie eine Abhängigkeit in diesem Dialogfeld aktivieren, teilen Sie der Softwareverteilung mit, keine weitere Aufforderung bzgl. dieser Abhängigkeit anzuzeigen. Sie können Abhängigkeiten aktivieren, von denen Sie wissen, dass sie auf verwalteten Geräten installiert sind. Dieses Dialogfeld dient nur Informationszwecken. Wenn eine Abhängigkeit auf einem Zielgerät fehlt und Sie diese Abhängigkeit nicht ausdrücklich als ein abhängiges Paket mit einbezogen haben, kann das RPM wahrscheinlich nicht fehlerfrei installiert werden.

Fehlerbehebung bei Verteilungsproblemen

Die Softwareverteilung hat den Vorteil, dass sie Pakete an eine große Anzahl von Geräten gleichzeitig verteilen kann. Wenn ein Paket Probleme bereitet oder es zwischen der Software, die verteilt wird, und bereits vorhandener Software Kompatibilitätsprobleme gibt, kann das bedeuten, dass Sie auf Tausenden von Geräten gleichzeitig Fehler verursachen. Wenn Sie eine Implementierung mithilfe der Softwareverteilung planen, sollte Sie deshalb überlegt vorgehen und darauf achten, dass der Helpdesk nicht von einer Flut von Supportanrufen überrollt wird.

Testen Sie vor der Verteilung eines neuen Pakets das Paket zunächst auf mehreren Testsystemen. Idealerweise sollten diese Testsysteme über alle Betriebssysteme und Anwendungen verfügen, die in Ihrer Umgebung verwendet werden. Nachdem Sie das Paket verteilt haben, sollten Sie sich vergewissern, dass alle Systeme und Anwendungen immer noch wie vorgesehen arbeiten.

Führen Sie, nachdem Testsysteme die Funktionstüchtigkeit des Pakets bestätigt haben, eine im Umfang begrenzte Verteilung durch. Wählen Sie als Ziel eine kleine Anzahl von Geräten in Ihrer Umgebung aus. Bei der Entscheidung, wie viele Geräte als Zielgeräte ausgewählt werden sollten, wird pauschal empfohlen, nicht mehr Geräte als Ziel auszuwählen, als Ihr Helpdesk unterstützen kann. Sobald das Paket an diese Geräte verteilt wurde, sollten Sie die Software ein paar Tage unangetastet lassen, um abzuwarten, ob Benutzer Probleme melden.

Nach dieser ersten limitierten Verteilung können Sie dann damit beginnen, die Software auf andere Geräte im Unternehmen zu übertragen. Die Geschwindigkeit, mit der diese Rollouts durchgeführt werden, sollte sich danach richten, über wie viele unterschiedliche Gerätetypen das Unternehmen verfügt und wie belastbar der Helpdesk ist.

Nähere Informationen finden Sie in der Benutzercommunity in folgendem Artikel über die Problembehebung bei der Softwareverteilung: http://community.landesk.com/support/docs/DOC-5096.

Verarbeitung von benutzerdefinierten Skripten für die Softwareverteilung

Benutzerdefinierte Skripts, die geplante Tasks steuern (**Extras > Verteilung > Geplante Tasks**) werden in drei Abschnitten verarbeitet:

- **Premachine:** Der Abschnitt "Premachine" des benutzerdefinierten Skripts wird zuerst und nur einmal am Beginn des Tasks verarbeitet. Verwenden Sie diesen Abschnitt für Tasks, die kein Zielgerät haben, und/oder für Targeted Multicast. Verwenden Sie im Premachine-Abschnitt des Skripts nur lokale Befehle, LOCxxx.

- **Rechner:** Die Befehle in diesem Abschnitt des Skripts werden als zweites und nur ein Mal pro Zielgerät ausgeführt. Diese Befehle können entweder Remote- oder lokale Ausführungsbefehle verwenden und werden in erster Linie für die Remoteausführung von SDCLIENT.EXE verwendet. Bevor die Befehle in diesem Abschnitt des Skripts abgearbeitet werden können, muss der SWD-Agent auf den Zielgeräten installiert werden.
- **Postmachine:** Dieser Abschnitt wird zuletzt und ebenfalls nur ein Mal verarbeitet, nachdem alle Geräte verarbeitet wurden. Die Softwareverteilung fügt keine Befehle zu diesem Abschnitt hinzu und unterstützt nur die lokalen Befehle LOCxxx. Die Befehle in diesem Abschnitt werden nicht verarbeitet, wenn Geräte, die im Task enthalten sind, diese Befehle nicht ausführen können. Das Skript InventoryScanner.ini, das mit Management Suite geliefert wird, enthält Einzelheiten über die Skriptbefehle

Benutzerdefinierte Skriptbefehle

Benutzerdefinierte Skripte unterstützen verschiedene lokale Befehle und Remotebefehle:

- **LOCEXEC:** Lokale Ausführung; mit diesem Befehl wird eine Anwendung auf dem lokalen Gerät (dies ist immer der Coreserver) ausgeführt.
- **LOCDEL:** Lokales Löschen; löscht eine Datei auf dem lokalen Gerät.
- **LOCMKDIR:** Lokale Ordnererstellung; erstellt einen Ordner auf dem lokalen Gerät.
- **LOCRD:** Lokale Ordnerlöschung; mit diesem Befehl wird ein Ordner auf dem lokalen Gerät gelöscht.
- **REMCOPY:** Remotekopie; kopiert eine Datei vom lokalen Gerät auf ein Remotegerät.
- **REMEXEC:** Remoteausführung; führt eine Anwendung auf dem angegebenen Remotegerät aus.
- **REMDEL:** Remotes Löschen; löscht eine Datei auf dem Remotegerät.
- **REMMKDIR:** Remote Ordnererstellung; erstellt einen Ordner auf dem Remotegerät.
- **REMRD:** Remote Ordnerlöschung; löscht einen Ordner auf dem Remotegerät.

HTTP- und UNC-Pfade in Skripten

Im Folgenden finden Sie Beispiele für Softwareverteilungs-.ini-Dateien, die die Unterschiede zwischen Skriptdateien für HTTP- und UNC-Pfad verdeutlichen.

HTTP-Pfadskriptdatei:

```
; Diese Datei wurde von Desktop Manager erstellt
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=http://<web server>/packages/test package.exe
-g={6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

UNC-Pfadskriptdatei:

```
; Diese Datei wurde von Desktop Manager erstellt
[MACHINES]
REMEXEC0=C:\Program Files\LANDesk\LDClient\sdclient.exe -p=\\sample_core\onefile\test package.exe -g=
{6DD454C0-11D3A0D1-a000B3B5-9BACBBC99CFC6D-9CE3504801A0D4B2FZ0829F08} -Ac -Ab
```

Beachten Sie, dass beide .ini-Dateien ähnliche Elemente enthalten. Im Abschnitt MACHINES bezeichnet die Option -P den Pfad, von dem das Gerät das Softwarepaket herunterlädt. Im HTTP-Beispiel ist der Pfad http://<web server>/packages/test package.exe.

Die nächste Option ist die Option -G; sie entspricht der GUID, einer eindeutigen Nummernkennung für jedes Paket. Diese nummerische Kennung wird von Package Builder generiert und hilft, Verwechslungen zwischen Paketen mit ähnlichen Namen bei der Installation zu verhindern.

Skriptleitfaden für Bereitstellungsskripte (.ini-Dateien)

Sie müssen nicht das Fenster **Dateibereitstellungsskript erstellen** verwenden, um die Bereitstellungsskriptdatei zu erstellen. Eine Bereitstellungsdatei ist eine .ini-Datei, die die Einstellungen enthält, die das Gerät für die Paketinstallation verwenden soll. Sie können eigene Verteilungsdateien in einem Texteditor wie Notepad erstellen, wenn Sie dies bevorzugen.

Eine .ini-Skriptdatei für die Softwareverteilung besteht aus folgenden Komponenten:

```
[MACHINES]
REMEXEC0=C:\Programme\LANDesk\LDClient\sdclient.exe
/p="http://computer_name/95Packages/Acro32_95.exe"
/g={281B46C0-11D3766F-a0008bab-F9751AC966F808-66E3BC2DF01A0D4B2F88670DE4}
/Ac
/N
```

REMEXEC0-Befehlsparameter

Die Parameter für den Befehl REMEXEC0 wurden in separate Zeilen eingefügt, um die Komponenten deutlicher hervorzuheben. In einer .ini-Datei muss sich der Befehl in einer Zeile befinden.

REMEXEC0 ist der Remoteausführungsbefehl. Wenn Sie mehr als einen REMEXEC0-Befehl in einer einzelnen Skriptdatei verwenden möchten, erhöhen Sie den Befehl bei jeder Verwendung. Wenn Sie z. B. drei REMEXEC-Aufrufe in einer .ini-Datei verwendet haben, sollten diese als REMEXEC0, REMEXEC1 und REMEXEC2 bezeichnet werden. Die Befehle müssen nicht inkrementiert werden, wenn sie sich in separaten Dateien befinden.

Der Parameter C:\Program Files\LANDesk\LDClient ist der korrekte Pfad zum SWD-Agenten.

Bedeutung der Softwareverteilungs-Fehlercodes

Allgemeine Informationen zur Fehlerbehebung bei Problemen mit der Softwareverteilung finden Sie auf der Website der LANDesk Benutzercommunity in folgendem Dokument:

- http://community.landesk.com/support/docs/DOC-5096

In der Konsole wird im rechten Fensterausschnitt des Fensters **Geplante Tasks** der Taskstatus angezeigt. Wenn Sie auf "Fehlgeschlagen" unter dem Task klicken, sehen Sie Geräte, auf denen der Auftrag misslungen ist, und damit verbundene Meldungen und Protokolle. Der Status und die Fehler werden in die folgenden Dateien protokolliert:

- Wenn der Fehler beim Versuch des Zugriffs auf das Paket aufgetreten ist, wird er in der Datei AICLIENT.LOG protokolliert.
- Wenn der Fehler bei der Verarbeitung des Pakets (z. B. beim Kopieren von Dateien) aufgetreten ist, wird er in der Datei INST32.LOG protokolliert.
- In der Datei SDCLIENT.LOG finden Sie allgemeine Übersichtsdaten zu jeder Installationsanforderung, die vom Coreserver empfangen wird.

Diese Protokolldateien werden auf dem jeweiligen Gerät gespeichert.

SDCLIENT.EXE Befehlszeilenschalter für die Softwareverteilung

Die Softwareverteilung wird durch ein Bereitstellungsskript vereinfacht. SDCLIENT.EXE verwaltet die Pakete mithilfe von Befehlszeilenschaltern aus der Skriptdatei, die an die Anwendung weitergegeben werden.

Nähere Informationen hierzu finden Sie in der Benutzercommunity in folgendem Artikel über SDCLIENT.EXE Befehlszeilenschalter: http://community.landesk.com/support/docs/DOC-13759.

Hilfe zur Softwareverteilung

Das Dialogfeld "Verteilungspaket"

Das Dialogfeld **Verteilungspaket** (**Extras > Verteilung > Verteilungspaket**) speichert Informationen in der Datenbank, die das Paket beschreiben, das Sie verteilen möchten. Die Daten enthalten die Einstellungen, die erforderlich sind, um ein bestimmtes Softwarepaket zu installieren (beispielsweise den Paketnamen, alle etwaigen Abhängigkeiten oder Voraussetzungen, Installationsoptionen usw.). Diese Informationen werden als "Verteilungspaket" bezeichnet.

Kopieren Sie das Paket auf Ihren Verteilungsserver, bevor Sie dieses Dialogfeld verwenden. Sie müssen nach dem Paket suchen und Informationen zu allen Paketvoraussetzungen oder zusätzlichen Dateien bereitstellen. Sobald Sie ein Verteilungspaket für Ihr Paket erstellt haben, können Sie es mit einer Verteilungsmethode (**Extras > Verteilung > Verteilungsmethoden**) auf Geräten bereitstellen.

Die Seite "Paketinformationen"

Diese Seite verwenden Sie, um den Paketnamen und die Primärdatei Ihres Pakets einzugeben. Wenn Ihr Paket aus nur einer Datei besteht, geben Sie sie hier ein. Wenn Ihr Paket mehrere Dateien umfasst, fügen Sie die Hauptdatei Ihres Pakets hinzu, beispielsweise die Datei, mit der die Installation gestartet wird. Sie können zusätzliche Unterstützungsdateien auf der Seite **Zusätzliche Dateien** hinzufügen.

Um den Dateibrowser zu verwenden, geben Sie eine Webfreigabe oder einen Dateipfad in das Feld neben der Schaltfläche **Ausführen** ein. Klicken Sie auf **Ausführen**, um das Ziel im Feld **Primärdatei** anzuzeigen. Dort können Sie mit dem Navigieren fortfahren. Doppelklicken Sie beim Suchen nach der Datei auf die Datei, die Sie als Primärdatei verwenden möchten. Hiermit wird der Dateiname zum Paketpfad neben der Schaltfläche "Ausführen" hinzugefügt.

- **Name:** Der Name, den Sie hier eingeben, wird in den Strukturansichten und Dialogfeldern der **Verteilungspakete** und **Verteilungsmethoden** angezeigt. Wählen Sie eine möglichst kurze Beschreibung, da Sie längere Beschreibungen mit der Bildlaufleiste einblenden müssen.
- **Beschreibung, die dem Endbenutzer beim Downloaden angezeigt werden soll:** Die Beschreibung, die Sie an dieser Stelle eingeben, wird in den Fenstern **Verteilungspakete** und **Verteilungsmethoden** und im Softwarebereitstellungsportal angezeigt.
- **Primärdatei:** Die Hauptdatei in diesem Paket.
- **Los:** Beginnt mit dem Durchsuchen des Pfads, den Sie neben der Schaltfläche "Los" eingegeben haben.
- **Nach oben:** Ruft, ausgehend von dem Speicherort, den Sie gegenwärtig durchsuchen, die nächsthöherer Ordnerebene ab.

Verwenden von Umgebungsvariablen

Unterstützung für das direkte Einfügen der Umgebungsvariablen in den Paketpfad ist in Management Suite nicht verfügbar; die Erweiterung kann jedoch nach wie vor mit benutzerdefinierten Skripten durchgeführt werden, die zu einem früheren Zeitpunkt erstellt wurden. Um Umgebungsvariablen für die neue SWD-Architektur zu unterstützen, sollte der Registrierungswert "PreferredPackageServer" auf die zu verwendende Umgebungsvariable gesetzt werden. Diese Umgebungsvariable wird dann erweitert, um den Server zu definieren, aus dem das Paket abgerufen werden sollte.

Die Seite "Installations-/Deinstallationsoptionen"

Auf dieser Seite geben Sie den Pakettyp an. Abhängig vom Paket, das Sie bereitstellen, stehen verschiedene Optionen zur Verfügung. Diese Optionen stehen nicht in allen Pakettypen zur Verfügung.

- **Installieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu installieren.
- **Deinstallieren:** Legt fest, dass Sie ein Installationspaket verwenden möchten, um die Software zu entfernen. Wenn diese Kennzeichnung festgelegt ist, entfernt das Skript alles, was mit dem Installationsskript installiert wurde.
- **Befehlszeile:** (Nicht verfügbar für SWD-, Macintosh- oder Linux-Pakete. Zeigt die Befehlszeile an, die an die angegebene Primärdatei übergeben wird. Die Softwareverteilung fügt die wichtigsten Parameter für den von Ihnen verteilten Pakettyp automatisch hinzu.

MSI-Installations-/Deinstallationsoptionen

MSI-Verteilungspakete bieten zusätzliche Installations-/Deinstallationsoptionen, wenn Sie **Windows-Installer verwenden, um die Installation durchzuführen und zu steuern (MSIexec).** auswählen.

- Anzeigeoptionen:
  - **Stiller Modus, keine Benutzerinteraktion:** Führt die Installation ohne Benachrichtigung auf dem verwalteten Gerät durch (Unbeaufsichtigte Installation).
  - **Unbeaufsichtigter Modus, nur Fortschrittsanzeige:** Zeigt während der Installation lediglich eine Fortschrittsanzeige, aber keine Optionen zum Abbrechen oder Verzögern an.

  • Legt die Ebene der Benutzerschnittstelle fest:

  - **Keine Benutzeroberfläche:** Führt eine vollständig unbeaufsichtigte Installation durch.
  - **Minimale Benutzeroberfläche:** Zeigt ein Vollbildfenster mit einer Fortschrittsanzeige und einer Schaltfläche "Abbrechen" an. Nach Abschluss der Installation wird ein Meldungsfeld angezeigt. Wenn Sie die Installation abbrechen, wird kein Meldungsfeld angezeigt.
  - **Reduzierte Benutzeroberfläche:** Zeigt nach Abschluss der Installation ein Meldungsfeld an.
  - **Vollständige Benutzeroberfläche:** Zeigt ein Vollbildfenster mit einer Fortschrittsanzeige und einer Schaltfläche "Abbrechen" an. Nach Abschluss der Installation wird ein Meldungsfeld angezeigt.
- Neustartoptionen:
  - **Nach Abschluss der Installation nicht neu starten:** Führt selbst dann keinen Neustart durch, wenn dieser von einer Installation durch harte Kodierung verlangt wird.
  - **Benutzer zum Neustart auffordern, falls erforderlich:** Fordert den Benutzer zum Neustart auf, wenn dies von der Installationsdatei verlangt wird.
  - **Den Computer nach der Installation immer neu starten:** Führt nach Abschluss der Installation einen Neustart durch.

- **Protokolldateiname:** Gibt den Speicherort und den Dateinamen für die Speicherung einer Windows Installer-Protokolldatei an, die auf der Basis der Installationsergebnisse nach Abschluss der Installation erstellt wird.
- **Protokollierungsoptionen:** Aktiviert die Erstellung der Protokolldatei, nachdem der Speicherort angegeben wurde.
- **Befehlszeile eingeben / oben Optionen auswählen und die Befehlszeile für MSI-Paket bearbeiten:** (Nicht verfügbar für SWD-Pakete) Zeigt die Befehlszeile an, die an die angegebene Primärdatei übergeben wird. Die Softwareverteilung fügt an dieser Stelle die Basisparameter zum Ändern des Standardverhaltens hinzu. Befehlszeilenfelder können auch unter Verwendung von Datenbankmakros Werte aus dem Inventar abrufen. Geben Sie die Inventarposition in %-Zeichen eingeschlossen an. Zum Beispiel:

  %Device_Name.Computer%

  Damit wird der Gerätename mit einem Unterstrich anstelle eines Leerzeichens angezeigt, und der Computer erscheint ganz oben in der Inventarstruktur.

Informationen zur Seite "Batchoptionen"

Die Optionen auf dieser Seite gelten für Pakete, die Skripte oder Batchdateien verwenden. Standardmäßig werden Pakete im 32-Bit-Modus ausgeführt. Dies bedeutet Folgendes:

- Wenn eine 32-Bit-Anwendung auf Registrierungswerte in HKEY_LOCAL_MACHINE\SOFTWARE zugreift, erfolgt der eigentliche Zugriff auf HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node.
- Wenn eine 32-Bit-Anwendung ein Programm unter c:\windows\system32 ausführt, dann wird eigentlich die 32-Bit-Version der Anwendung von C:\Windows\SysWOW64 aus ausgeführt. Hierzu zählen cmd.exe, cscript.exe, wscript.exe und andere.

Wenn Sie **Als 64-Bit-Anwendung auf 64-Bit-Windows ausführen** auswählen, geschieht Folgendes mit Skripten und Batchdateien:

- Lesen und Schreiben erfolgt nach HKEY_LOCAL_MACHINE\SOFTWARE anstelle von HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node
- Sie starten die 64-Bit-Anwendungen von System32 und nicht die 32-Bit-Anwendungen (unter c:\windows\SysWOW64).

Weitere Informationen von Microsoft zum Ausführen von 32-Bit-Anwendungen in einer 64-Bit-Umgebung finden Sie auf folgender MSDN-Seite:

- http://msdn.microsoft.com/en-us/library/aa384249(VS.85).aspx

Informationen zur Seite "Optionen für die Clientwarteschlange"

Die Seite "Optionen für die Clientwarteschlange" verwenden Sie, um die Verarbeitung gleichzeitiger Verteilungsaufträge zu konfigurieren.

Dank der Clientwarteschlange kann jeder Client mehrere gleichzeitige Aufträge in der Reihenfolge ihres Eingangs abarbeiten, wobei pushbasierte Aufträge Priorität haben.

Die Aufträge werden zwar immer noch der Reihe nach verarbeitet, aber die Warteschlange gestattet die Ausführung mehrerer Aufträge, anstatt für eingehende Aufträge einen Fehler auszugeben, wenn bereits ein Auftrag aktiv ist.

- **Einstellen in die Clientwarteschlange deaktivieren:** Deaktiviert das Einstellen in die Warteschlange für das aktuelle Paket. Wenn andere Aufträge auf einem Gerät aktiv sind und das betreffende Gerät diesen Auftrag erhält, dann schlägt der Auftrag fehl.

Die Seite "Zusätzliche Dateien"

Wenn Ihr Paket aus mehreren Dateien besteht, können Sie diese auf dieser Seite hinzufügen. Um den Dateibrowser zu verwenden, geben Sie eine Webfreigabe oder einen Dateipfad in das Feld neben der Schaltfläche "Los" ein. Mit der Schaltfläche "Los" wird das Ziel im Feld **Verfügbare Dateien** angezeigt. Dort können Sie mit dem Navigieren fortfahren. Wählen Sie Dateien im Feld **Verfügbare Dateien** aus und klicken Sie auf **>>**, um sie zur Liste **Zusätzliche Dateien** hinzuzufügen. Hiermit werden die Dateien zum Paket hinzugefügt.

- **Automatische Erkennung:** Diese Option ist für MSI-Pakete verfügbar. Sie durchsucht die primäre MSI-Datei auf externe Dateireferenzen und fügt diese automatisch hinzu.
- **Pfeile:** Mit diesen Pfeilen werden ausgewählte Dateien zur Liste **Zusätzliche Dateien** hinzugefügt bzw. daraus entfernt.
- **Schaltfläche "Los":** Beginnt mit dem Durchsuchen des Pfads, den Sie neben der Schaltfläche "Los" eingegeben haben.
- **Schaltfläche "Nach oben":** Ruft, ausgehend von dem Speicherort, den Sie gegenwärtig durchsuchen, die nächsthöherer Ordnerebene ab.

Die Seite "Abhängige Pakete"

Abhängige Pakete sind Pakete, die sich bereits auf dem Gerät befinden müssen, damit sich das Paket, an dessen Konfiguration Sie gerade arbeiten, installieren lässt. Wenn keine abhängigen Pakete auf dem Gerät vorhanden sind, werden diese automatisch installiert. MSI- und SWD-Pakete werden automatisch über die entsprechenden Registrierungsschlüssel auf dem Gerät erkannt. Bei anderen Pakettypen hängt die Paketerkennungsmethode davon ab, was Sie auf der Erkennungsseite auswählen.

Wenn Sie ein vorhandenes Paket, das über eine Abhängigkeit verfügt, dem von Ihnen erstellten Paket als abhängiges Paket hinzufügen, wird diese vorhandene Abhängigkeit auch dem neuen Paket hinzugefügt.

- **Verfügbare Pakete:** Listet die Pakete auf, die Sie mithilfe des Fensters **Verteilungspakete** erstellt haben. Nur öffentliche Pakete können abhängige Pakete sein. Wählen Sie die Pakete aus, die Sie als abhängige Pakete definieren möchten, und klicken Sie auf **>>**.
- **Abhängige Pakete:** Listet die Pakete auf, die Sie als abhängige Pakete ausgewählt haben.
- **Pfeile:** Mit diesen Pfeilen werden ausgewählte Dateien zur Liste **Zusätzliche Dateien** hinzugefügt bzw. daraus entfernt.
- Schaltflächen **Nach oben** und **Nach unten**: Abhängige Pakete werden in der Reihenfolge angewendet, in der sie in der Liste **Abhängige Pakete** erscheinen. Die Schaltflächen **Nach oben** und **Nach unter** verwenden Sie, um die Abfolge der abhängigen Pakete anzupassen.

Erläuterungen zu den Linux-Software-Abhängigkeiten

Wenn Sie im Dialogfeld **Verteilungspakete - Eigenschaften** eines Linux-Pakets auf **Speichern** klicken, analysiert die Softwareverteilung den primären RPM und alle von Ihnen ausgewählten abhängigen RPMs auf Abhängigkeiten, die die RPMs erfordern. Diese Abhängigkeiten werden dann im Dialogfeld **Fehlende Bibliotheken** angezeigt. Wenn Sie eine Abhängigkeit in diesem Dialogfeld aktivieren, teilen Sie der Softwareverteilung mit, keine weitere Aufforderung bzgl. dieser Abhängigkeit anzuzeigen. Sie können Abhängigkeiten aktivieren, von denen Sie wissen, dass sie auf verwalteten Geräten installiert sind. Dieses Dialogfeld dient nur Informationszwecken. Wenn eine Abhängigkeit auf einem Zielgerät fehlt und Sie diese Abhängigkeit nicht ausdrücklich als ein abhängiges Paket mit einbezogen haben, kann das RPM wahrscheinlich nicht fehlerfrei installiert werden.

Die Seite "Anforderungen"

Mit der Seite "Anforderungen" können Sie Anforderungen für die Paketinstallation definieren. Sie können dies über eine Abfrage oder eine zusätzliche Datei/Anwendung durchführen, die auf Geräten ausgeführt wird und einen Errorlevel-Code zurückgibt. Ein Non-Zero-Code verhindert, dass das Paket installiert wird.

Anforderungen werden auf Geräten in der Zielliste ausgeführt. Wenn ein Gerät in der Zielliste eine bestimmte Anforderung nicht erfüllt, wird das Paket auf diesem Gerät nicht installiert. Die Fehlerdetails werden im Protokoll des Verteilungstasks aufgezeichnet.

Anforderungen sind ein praktisches Hilfsmittel in Unternehmen, in denen die Paketerstellung und die Paketverteilung von unterschiedlichen Personen gehandhabt wird. Die Person, die für die Paketverteilung zuständig ist, ist möglicherweise nicht mit den Systemanforderungen des Pakets vertraut, die dem Paketersteller bekannt sind. In diesen Fällen kann der Paketersteller eine Abfrage erstellen, die Paketanforderungen (z.B. Betriebssystem und Speichervolumen) einschließt.

Für die Option zum Hinzufügen einer zusätzlichen Datei können Sie eine Datei auswählen, die in der Liste "Zusätzliche Dateien" des Pakets enthalten ist. Anschließend können Sie dann die Befehlszeile angeben, mit der die Datei ausgeführt werden soll.

- **Abfrage auswählen:** Wählen Sie eine vorhandene Abfrage aus, die Sie zum Filtern von Zielgeräten verwenden möchten. Sie können auch auf **Abfrage erstellen** klicken, um eine neue Abfrage zu erstellen.
- **Zusätzliche Datei ausführen:** Aktivieren Sie diese Option, wenn Sie eine Datei auf den Geräten ausführen möchten.
- **Zusätzliche Datei auswählen:** Geben Sie die Datei ein, die von den Geräten ausgeführt werden soll. Diese Datei wird vor allen anderen Paketdateien ausgeführt.
- **Befehlszeile:** Wenn die von Ihnen angegebene Datei eine Befehlszeile benötigt, geben Sie sie hier ein.

Die Seite "Erkennung"

Die Seite "Erkennung" verwenden Sie, um zu konfigurieren, wie bei der Softwareverteilung erkannt wird, ob ein Paket bereits bereitgestellt wurde. Die Seite "Erkennung" steht nur für ausführbare Pakete, Batchdateipakete und Pakete mit virtualisierter Anwendung zur Verfügung. Eine Übereinstimmung mit einem Kriterium/mehreren Kriterien verhindert, dass abhängige Pakete installiert werden.

Die folgenden Erkennungsmethoden können verwendet werden:

- **Erkannt von:** Bestimmt, ob ein Paket bereits installiert wurde, indem geprüft wird ob eines der folgenden Kriterien erfüllt ist:

    - Datei existiert
    - Dateiversion
    - Dateigröße und/oder Prüfsumme
    - Dateidatum
    - Registrierungsschlüssel existiert
    - Registrierungswert existiert
    - Passender Registrierungswert
- **Dateipfad:** Gibt den Speicherort und Namen des zu erkennenden Elements an.
- **Rekursiv nach der Datei suchen:** Kaskadiert eine Suche durch die Unterverzeichnisse des Verzeichnisses, das im Feld **Dateipfad** angegeben wurde.

Sie können mehrere Kriterien hinzufügen, indem Sie diese angeben und dann auf die Schaltfläche **Hinzufügen** klicken.

Die MSI- und SWD-Pakete stellen GUIDs im Rahmen ihrer Installationen bereit. Diese werden verwendet, um zu bestimmen, ob ein Paket bereits installiert ist. Die Erkennungsoption steht für diese Pakettypen nicht zur Verfügung.

Die Seite "Konten"

Auf der Seite "Konten" können Sie den Typ des Benutzerkontos auswählen, das für die Verteilung der Pakete verwendet werden soll.

- **LocalSystem-Konto:** Das Konto des Geräts.
- **Konto des aktuellen Benutzers:** Das Konto des aktuellen Benutzers. Es muss ein Benutzer beim Gerät angemeldet sein, sonst schlägt der Paketverteilungstask fehl.
- **Ausführen als ein bestimmter Benutzer:** Das von Ihnen festgelegte Konto eines Benutzers. Sie müssen eine\n **Domäne\Benutzernamen** und ein **Kennwort** für den Benutzer angeben, den Sie verwenden möchten.

Verwenden der Seite "Timeout-Einstellungen"

Auf der Seite "Timeout-Einstellungen" können Sie einen Timeout.für die Installation definieren.

- **Timeout für Paketinstallation aktivieren:** Gibt bei Auswahl die Anzahl der Stunden an, die Sie für die Paketinstallation zulassen. Ist das Paket beim Erreichen des Zeitlimits nicht installiert, gilt der Auftrag als fehlgeschlagen.

Verwenden der Seite "Assoziation deinstallieren"

Mithilfe der Seite "Assoziation deinstallieren" können Sie ein Deinstallationspaket für ein Richtlinienpaket der Softwarebereitstellung zuordnen. Dadurch wird die Software automatisch vom Client gelöscht, wenn das Gerät oder der Benutzer von der Zielliste oder Abfrage entfernt wird. **HINWEIS:** Deinstallationspakete werden nur mit richtlinienbasierter Bereitstellung verwendet.

- **Typ:** Wählen Sie den Pakettyp aus, der zur Deinstallation des Pakets verwendet werden soll. In der Liste "Verfügbare Verteilungspakete:" werden nur Pakete des von Ihnen definierten Typs angezeigt.
- **Aktuell:** Das derzeit ausgewählte Paket.

Die Seite "Rückgabecodes zuweisen"

Die Seite **Rückgabecodes zuweisen** verwenden Sie, um Verteilungspaket-Statusmeldungen zu konfigurieren, die anhängig davon, ob ein Verteilungstask erfolgreich oder nicht erfolgreich abgeschlossen wurde, in der Konsole angezeigt werden.

Die Seite **Rückgabecodes zuweisen** bietet die folgenden Optionen:

- **Paketinformationen:** Enthält eine Zusammenfassung der Eigenschaften für das Verteilungspaket.
  - **Paketname:** Zeigt den Namen des Verteilungspakets an.
  - **Pakettyp:** Zeigt den Pakettyp an (MSI, EXE, BAT, etc.).
  - **Zugewiesene Vorlage:** Zeigt die Rückgabecodevorlage an, die mit diesem Verteilungspaket verknüpft wurde.
- **Rückgabecodevorlagen-Informationen:** Zeigt den Namen, die Beschreibung und das Änderungsdatum für alle verfügbaren Vorlagen an. Wenn Sie eine bestimmte Vorlage mit einem Verteilungspaket verknüpfen wollen, klicken Sie zunächst auf die Vorlage und dann auf die Schaltfläche **Zuweisen**.
- **Ändern:** Ändert die Vorlage und ruft das Fenster "Paket-Rückgabecodezuordnungen" auf.
- **Zuweisen:** Verknüpft die derzeit ausgewählte Vorlage mit dem Verteilungspaket.

Die Rückgabecode-Vorlagenverwaltung

Die **Rückgabecode-Vorlagenverwaltung** verwenden Sie zum Hinzufügen, Ändern, Löschen, Importieren und Exportieren von Rückgabecodevorlagen. Sie können dieses Dialogfeld vom Extra "Verteilungspakete" aus aufrufen, indem Sie auf die Symbolleistenschaltfläche **Rückgabecode-Vorlagenverwaltung** klicken. Das Dialogfeld **Rückgabecode-Vorlagenverwaltung** bietet die folgenden Optionen:

- **Rückgabecodevorlagen-Informationen:** Listet alle vorhandenen Vorlagen nach Namen, Beschreibung, Typ und Änderungsdatum auf.
- **Vorlagenfiltertyp:** Filtert die Liste der Vorlagen, so dass "Alle", "MSI" oder "Sonstige" Vorlagen angezeigt werden.
- **Name der Vorlage:** Zeigt den Namen an, der der neuen Vorlage zugewiesen werden soll.
- **Vorlagenbeschreibung:** Zeigt die Beschreibung an, die der neuen Vorlage zugewiesen werden soll.
- **Vorlagenfiltertyp**: Zeigt die Gruppe an, der die neue Vorlage zwecks Filteroptionen zugewiesen wird. Wählen Sie zwischen MSI und Sonstige.
- **Hinzufügen:** Öffnet das Fenster "Neue Rückgabecode-Zuordnungsvorlage".
- **Ändern:** Öffnet das Fenster "Paket-Rückgabecodezuordnungen", in dem der Benutzer die ausgewählte Vorlage ändern kann.
- **Löschen:** Entfernt die ausgewählte Vorlage.
- **Importieren:** Ermöglicht den Import einer Vorlage von einem definierten Speicherort (.xml-Format).
- **Exportieren:** Ermöglicht den Export einer Vorlage von einem definierten Speicherort (.xml-Format).

Das Dialogfeld "Paket-Rückgabecodezuordnungen"

Das Fenster "Paketrückgabecodezuordnung" bietet die folgenden Optionen:

- **Rückgabecodevorlagen-Informationen:** Listet die allgemeinen Eigenschaften der Vorlage auf.
  - **Name der Vorlage:** Zeigt den Namen der Vorlage an, die in der Rückgabecode-Vorlagenverwaltung zugewiesen wurde.

    - **Vorlagenbeschreibung:** Zeigt die Beschreibung der Vorlage an, die in der Rückgabecode-Vorlagenverwaltung zugewiesen wurde.
- **Standardverhalten:**
    - **Status:** Weist einen Status "erfolgreich" oder "nicht erfolgreich" zu.
    - **Meldung:** Dient der Eingabe einer benutzerdefinierten Meldung, die angezeigt wird, falls ein Paket den ausgewählten Rückgabecode zurücksendet.
- **Rückgabecodezuordnungen:** Weist neue Rückgabecodes zu oder entfernt vorhandene Rückgabecodes unter Verwendung der Schaltflächen **Hinzufügen** oder **Löschen** (auf der rechten Seite). Auf diese Weise hinzugefügte Rückgabecodes werden in numerischer Folge erstellt.
- **Rückgabecodezuordnung bearbeiten:** Dient der Eingabe der Nummer(n) für die zu erstellenden Rückgabecodes. Wenn Sie Ihre Hinzufügungen und Änderungen in diesem Bereich abgeschlossen haben, klicken Sie auf die Schaltfläche **Übernehmen**.
    - **Einzelne:** Ermöglicht die Zuweisung einer einzelnen Rückgabecodenummer, die dann einem Status und einer benutzerdefinierten Meldung zugewiesen werden kann.
    - **Bereich:** Ermöglicht die Zuweisung eines Bereichs von Rückgabecodenummern, die dann demselben Status und derselben benutzerdefinierten Meldung zugewiesen werden können.
- **Meldung:** Die benutzerdefinierte Meldung, die angezeigt wird, wenn das Paket den Rückgabecode zurücksendet.
- **Status:** Legt fest, ob der Rückgabecode Erfolg oder Misserfolg signalisiert.

Die Seite "SWD-Paketoptionen"

Auf dieser Seite legen Sie fest, was geschieht, wenn ein SWD-Paket bereits auf einem Gerät installiert ist. Wenn Anwendungen vorhanden sind, die nicht auf eine normale Paketreparatur reagieren, ist die Option für eine komplette Neuinstallation möglicherweise besser geeignet. Reparaturen sind in der Regel weniger zeitaufwendig als eine komplette Neuinstallation.

Sie können SWD-Pakete mit oder ohne eine für die Benutzer sichtbare Paketinstallationsoberfläche erstellen. Wenn das Paket eine Oberfläche hat, können Sie festlegen, ob das Dialogfeld des Paketinstallationsstatus über den vorhandenen Anwendungen der Benutzer angezeigt wird oder ob ein blauer Installationshintergrund zu sehen sein soll, der den Desktop verdeckt, während das Paket installiert wird.

- **Das Paket reparieren:** Durch diese Option werden die Registrierungsschlüssel nur aktualisiert und nur die Programmdateien, die der Agent als abweichend von den Dateien im Installationspaket erkennt, ersetzt.
- **Vollständige Neuinstallation des Pakets durchführen:** Durch diese Option wird das Paket komplett neu installiert, alle Dateien ersetzt und alle Registrierungsschlüssel neu erstellt.
- **Wenn Feedback aktiviert ist, überschreiben Sie die obige Einstellung und lassen Sie den Benutzer entscheiden:** Hiermit können Benutzer zwischen Reparatur oder Neuinstallation entscheiden. Sie können Feedback auf der Seite **Feedback** des Dialogfelds **Verteilungsmethode - Eigenschaften** aktivieren.
- **Wenn 'Feedback' aktiviert ist, Hintergrundbildschirm anzeigen:** Blendet den einfarbigen blauen Hintergrundbildschirm ein. Sie können Feedback auf der Seite **Feedback** des Dialogfelds **Verteilungsmethode - Eigenschaften** aktivieren.

Das Dialogfeld "Verteilungsmethoden"

Das Dialogfeld **Verteilungsmethoden** (**Extras > Verteilung > Verteilungsmethoden**) legt fest, wie ein Paket an Geräte gesendet wird. Diese Optionen sind nicht mit einem bestimmten Verteilungspaket verknüpft. Die Optionsauswahl umfasst Targeted Multicast- und Push- oder Pull-basierte Verteilungen. Definieren Sie nicht jedes Mal, wenn Sie ein Paket verteilen möchten, eine Verteilungsmethode. Idealerweise erstellen Sie eine Vorlage für Liefermethoden, die sich für Verteilungen, bei denen dieselbe Verteilungsmethode zum Einsatz kommt, erneut verwenden lässt.

Erstellen Sie vor dem Verwenden dieses Dialogfelds das Verteilungspaket (**Extras > Verteilung > Verteilungspakete**), das Sie bereitstellen möchten.

Die Seite "Beschreibung"

Diese Seite verwenden Sie, um die von Ihnen konfigurierte Verteilungsmethode zu beschreiben und um festzulegen, an wie viele Geräte die Verteilung gleichzeitig erfolgen soll.

- **Name:** Der Name Ihrer Verteilungsmethode.
- **Eigentümer:** Der Name der Person, die das Paket ursprünglich erstellt hat. Dieses Feld kann von Ihnen nicht geändert werden.
- **Beschreibung der Verteilungsmethode:** Die Beschreibung, die Sie hier eingeben, wird in den Strukturansichten und Dialogfeldern der **Verteilungspakete** und **Verteilungsmethoden** angezeigt. Wählen Sie eine möglichst kurze Beschreibung, da Sie längere Beschreibungen mit der Bildlaufleiste einblenden müssen.
- **Anzahl der zu verteilenden Computer:** Steuert die maximale Anzahl von Geräten, die die Softwareverteilung gleichzeitig erhalten können.

Informationen zur Seite "Netzwerkverwendung"

Diese Seite verwenden Sie, um zu steuern, wie das Paket und die Paketdateien an verwaltete Geräte gesendet werden. Die folgenden Optionen stehen Ihnen zur Verfügung:

- **Dateien mit Multicast bereitstellen:** Verwendet Targeted Multicast, um Dateien an mehrere Geräte gleichzeitig zu senden.
- **Dateien mit 'Ausführen aus Quelle' bereitstellen:** Kopiert keine Dateien lokal, bevor sie installiert werden. Stattdessen wird die primäre Paketdatei direkt aus dem Downloadspeicherort des Pakets ausgeführt. Diese Option wird von allen Pakettypen auf UNC-Paketfreigaben unterstützt. Von HTTP-Freigaben wird diese Option nur für SWD- und MSI-Pakettypen unterstützt. Sie können diese Option mit Programminstallationen verwenden, die eine spezifische Ordnerstruktur erfordern. Diese Option arbeitet mit bevorzugten Servern, jedoch versucht sie nicht, das Paket von einem Peer auszuführen.
- **Dateien mit 'Download aus der Quelle' bereitstellen:** Geräte laden Paketdateien aus dem Paketserver, bevor sie die Dateien verwenden. Diese Option nutzt nicht die Vorteile von Targeted Multicast.

Informationen zur Seite "Bandbreite" (unter der Seite "Netzwerkverwendung")

Über diese Seite können Sie die Netzwerkbandbreite steuern, die das Paket für die Bereitstellung erfordert. Sie müssen keine dieser Optionen auswählen, wenn Sie möchten, dass alle ausgewählten Geräte das Paket unabhängig von ihrer Bandbreite erhalten.

Die Bandbreitensteuerung ist wichtig für Geräte mit einer langsamen WAN- oder Einwählverbindung. In der Regel werden Sie keine Multimegabyte-Pakete über langsame Verbindungen auf Geräten bereitstellen wollen. Wählen Sie eine der folgenden Optionen aus:

- **Eine Nicht-RAS-Netzwerkverbindung erfordern:** Diese Option aktiviert die Bandbreitenvoraussetzung. Wählen Sie eine der folgenden Optionen:
  - **Alle Nicht-RAS-Netzwerkverbindungen zulassen:** Diese Option aktiviert WAN- und LAN-Geräte für den Empfang des Pakets.
  - **Hochgeschwindigkeitsverbindung erforderlich:** Diese Option aktiviert nur LAN-Geräte für den Empfang des Pakets.
- **Remotedownloaden (pro Subnetz) auf jeweils ein Gerät limitieren:** Reduzieren Sie mit dieser Option die in einem Subnetz beanspruchte Bandbreite.
  - **Maximaler Prozentsatz an Bandbreite:** Wenn Sie die Option zur Limitierung von Remotedownloads ausgewählt haben, können Sie den Bandbreitenkonsum zusätzlich einschränken, indem Sie den vom Zielgerät für diese Verteilung maximal zu verwendenden Prozentsatz an Netzwerkbandbreite anpassen.

Wenn Sie PDS zum Erkennen der Netzwerkgeschwindigkeit verwenden, geben Hochgeschwindigkeits- und langsame Verbindungen dieselben Daten zurück. Sie müssen ICMP verwenden, damit Hochgeschwindigkeits-Netzwerkverbindungen richtig erkannt werden.

ICMP sendet ICMP-Echoanforderungen verschiedener Größe an die Remotecomputer und verwendet die Antwortzeit dieser Echoanforderungen bzw. -reaktionen zur Bestimmung der ungefähren Bandbreite. Allerdings unterstützen nicht alle Router oder Computer das Weiterleiten oder Beantworten von ICMP-Echoanforderungen. ICMP unterscheidet auch zwischen Hochgeschwindigkeitsverbindungen (LAN) und langsamen Verbindungen (WAN), wobei es sich bei letzteren jedoch nicht um Einwählverbindungen handelt.

Wenn Ihre Netzwerkkonfiguration keine ICMP-Echoanforderungen zulässt, können Sie PDS wählen. Wenn Sie PDS verwenden, gibt Ihnen die Option **Hochgeschwindigkeitsverbindung erforderlich** keine exakte Steuerung.

Informationen zur Seite "Bandbreitenverwendung" (unter der Seite "Netzwerkverwendung")

Auf dieser Seite konfigurieren Sie die Bandbreitendrosselung und Paketverzögerungen.

- **Peer-Download (nur vom Cache oder Peer installieren):** Ist unter Umständen nicht in allen Dialogfeldern **Bandbreitenverwendung** sichtbar. Lässt einen Download von Paketen nur dann zu, wenn sie sich im lokalen Cache oder auf einem Peer in der gleichen Multicast-Domäne befinden. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer befindet.
- **Vom Core oder bevorzugten Server genutzte Bandbreite (WAN):** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. WAN-Verbindungen sind in der Regel langsamer, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen niedrigeren Prozentsatz einzustellen.
- **Von Peer zu Peer genutzte Bandbreite (lokal):** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. LAN-Verbindungen sind in der Regel schneller als WAN-Verbindungen, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen höheren Prozentsatz einzustellen, als den Prozentsatz für WAN.

Informationen zur Seite "Multicast-Domänen" (unter der Seite "Netzwerkverwendung")

Diese Seite wird nur angezeigt, wenn Sie "Multicast" als Verteilungstyp ausgewählt haben. Auf dieser Seite konfigurieren Sie Multicast-Optionen.

- **Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Task durchzuführen. Bei dieser Option werden die Domänenerkennungsergebnisse für die erneute Verwendung nicht gespeichert.
- **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Task durchzuführen und die Ergebnisse für eine künftige Verwendung zu speichern; somit sparen Sie Zeit bei folgenden Multicasts
- **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option immer dann, wenn Sie durch Targeted Multicast eine Domänenerkennung durchgeführt haben und speichern Sie die Ergebnisse.
- **Domänenrepräsentanten reaktivieren verwaltete Geräte:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan"-Technologie unterstützen, beim Empfang von Multicast einschalten möchten. Mit dem Dialogfeld "Multicast-Optionen" können Sie festlegen, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das "Wake on Lan"-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden.
- **Wartezeit nach WOL-Versuch (Sek.):** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Informationen zur Domänenerkennung

Die Domänenerkennung ist nur auf Netzwerken mit Subnetzen erforderlich, die gegenseitig ihren Multicast-Datenverkehr erkennen können. Wenn Ihre Subnetze den gegenseitigen Datenverkehr nicht erkennen, können Sie Zeit sparen, indem Sie zuerst die Ergebnisse einer Domänenerkennung speichern und dann die Option **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** auswählen; Targeted Multicast muss dann nicht vor jedem Task eine Domänenerkennung durchführen.

Erkennen Ihre Netzwerksubnetze den gegenseitigen Multicast-Datenverkehr jedoch, so können Sie die Leistung von Targeted Multicast beschleunigen, indem Sie die Domänen vorab mithilfe des Skripts multicast_domain_discovery.ini identifizieren, das sich im Verzeichnis ManagementSuite\Scripts befindet. Dieses Skript führt auf Zielgeräten keine Vorgänge aus. Führen Sie dieses Skript im Fenster **Geplante Tasks** für eine Liste mit Zielen aus, die Ihr gesamtes Netzwerk umspannt. Die Domänenerkennungsergebnisse werden dadurch für die künftige Verwendung gespeichert. Sie können dieses Skript regelmäßig vor großvolumigen Multicast-Verteilungen ausführen.

Wenn Sie **Cachedatei verwenden** unter **Konfigurieren > Dienste > Multicast** ausgewählt haben, durchläuft Targeted Multicast einen Erkennungsvorgang, auch wenn Sie **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** ausgewählt haben. Targeted Multicast muss dies durchführen, um herauszufinden, welche potenziellen Multicast-Domänenrepräsentanten die Datei in ihrem Cache gespeichert haben.

Informationen zur Seite "Multicastlimits" (unter der Seite "Netzwerkverwendung")

Auf dieser Seite konfigurieren Sie taskspezifische Targeted Multicast-Parameter. Die Standardwerte in diesem Dialogfeld sind in der Regel für die meisten Multicasts geeignet.

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Die Zahl der Repräsentanten, die aktiv zur selben Zeit einen Multicast durchführen, ist auf diese Anzahl beschränkt. Standard ist 5.
- **Maximale Anzahl von Geräten, deren gleichzeitige Multicast-Verarbeitung misslungen ist:** Wenn ein Gerät die Datei über Multicast nicht erhält, lädt es die Datei aus dem Web oder vom Dateiserver herunter. Dieser Parameter kann verwendet werden, um die Anzahl der Geräte zu beschränken, die die Datei gleichzeitig erhalten. Wenn z. B. die Thread-Höchstzahl 200 war und die Höchstzahl der fehlgeschlagenen Multicast-Threads bei 20 lag, würde der "Geplante Task"-Handler nicht mehr als 20 Computer, bei denen Multicast fehlgeschlagen ist, gleichzeitig verarbeiten. Der "Geplante Task"-Handler verarbeitet bis zu 200 Geräte gleichzeitig, wenn diese erfolgreich den Multicast erhalten haben; jedoch nur maximal 20 der 200 Threads verarbeiten Geräte, bei denen der Multicast-Task misslungen ist. Wenn dieser Wert auf 0 gesetzt wurde, verarbeitet der "Geplante Task"-Handler den Verteilungsabschnitt des Task für keinen der Computer, auf dem Multicasting misslungen ist. Standard ist 240.
- **Speicherzeitraum für Dateien im Gerätecache:** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache des jeweiligen Zielcomputers gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht. Standard ist 2.
- **Speicherzeitraum für Dateien im Multicast-Domänenrepräsentanten-Cache (Tage):** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache auf dem Multicast-Domänenrepräsentanten gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht. Standard ist 14.

Die Seite "Neu starten"

Auf dieser Seite legen Sie fest, ob der Computer neu gestartet wird, nachdem die Software installiert oder deinstalliert wurde. Es stehen Ihnen drei Optionen zur Verfügung:

- **Nur bei Bedarf neu starten:** Geräte werden neu gestartet, wenn es das Paket verlangt.
- **Nie neu starten:** Geräte werden nach einer Paketinstallation nicht neu gestartet. Wenn Sie diese Einstellung auswählen und das Paket einen Neustart erforderlich macht, kann es auf den Geräten zu Fehlern bei der Programmausführung kommen, sofern kein Neustart durchgeführt wird. Wenn es sich bei dem Paket um ein SWD-Paket handelt, überschreibt diese Option alle Einstellungen im Paket. Wenn es sich bei dem Paket um eine generische ausführbare Datei oder um ein MSI-Paket handelt, überschreibt die Paketeinstellung möglicherweise diese Option.
- **Immer neu starten:** Geräte werden neu gestartet, unabhängig davon, ob es das Paket verlangt oder nicht.

Informationen zur Seite "Feedback und Timing"

Diese Seite verwenden Sie, um zu entscheiden, wie viel dem Benutzer während der Installation oder der Deinstallation der Software angezeigt wird. Die folgenden Optionen stehen Ihnen zur Verfügung:

- **Benutzerschnittstelle für Paketfortschritt:**
  - **Kein Feedback anzeigen:** Verbirgt die Installation gegenüber dem Benutzer in dem Maße, wie es die Softwareverteilungspakete erlauben. Diese Option ist davon abhängig, ob das Softwareverteilungspaket für eine unbeaufsichtigte Installation erstellt wurde.
  - **Fortschritt auf dem Bildschirm des Benutzers anzeigen:** Aktiviert das Meldungsfeld für die Benachrichtigung über die Softwareinstallation und die Animation des Taskleistensymbols während der Softwareinstallation. Darüber hinaus werden die folgenden Optionen aktiviert:
- **Das Paket sofort ausführen:** Installiert das Paket, ohne Verzögerungsoptionen zuzulassen.

- **Zulassen, dass der Benutzer die Paketausführung verzögern darf:** Aktiviert Optionen, mit denen Benutzer Paketinstallationen verzögern können. Dies kann hilfreich sein, wenn Benutzer gerade einen Task ausführen, der durch die Installation gestört werden könnte.
    - **Bis zur nächsten Anmeldung automatisch verzögern:** Wenn diese Option aktiviert ist, wird die Paketinstallation bis zur nächsten Anmeldung verschoben, ohne dass eine Eingabeaufforderung für den Benutzer angezeigt wird. Wenn Sie **Benutzer wählt die Verzögerungszeitspanne aus** aktivieren, wird nach der nächsten Anmeldung das Verzögerungsdialogfeld angezeigt.
    - **Benutzer vor dem Downloaden des Pakets fragen:** Benachrichtigt den Benutzer, bevor ein verwaltetes Gerät den Download des Pakets initiiert. Diese Option ist insbesondere für mobile Benutzer nützlich, wenn sie in Verbindung mit Verzögerungsoptionen verwendet wird, um einen Benutzer davor zu bewahren, eine umfangreiche Anwendung über eine langsame Verbindung herunterladen zu müssen.
    - **Benutzer fragen, bevor Paket ausgeführt wird.** Zeigt eine Meldung an, bevor die Installation nach dem Download des Pakets in den lokalen Verteilungscache gestartet wird.
- **Benutzer darf abbrechen:** Diese Option ermöglicht es dem Benutzer, die Aktion (Installation oder Deinstallation) abzubrechen: Diese Option wird nicht für Anwendungsrichtlinien empfohlen.
- **Vollständige Paketoberfläche anzeigen:** Diese Option steuert, ob das Paket im Hintergrund installiert wird (deaktiviert) oder ob es nach Bedarf Eingabeaufforderungen für den Benutzer einblendet (aktiviert).
- **Erfolgs- oder Fehlerstatus dem Endbenutzer anzeigen:** Zeigt nach der Installation des Pakets ein Dialogfeld an, das den Benutzer informiert, ob die Installation erfolgreich war oder nicht.

Informationen zur Seite "Weitere Verzögerungsoptionen" (unter der Seite "Feedback und Timing")

Diese Seite verwenden Sie zum Konfigurieren von Paketverzögerungslimits und Timeoutoptionen. Die Optionen auf dieser Seite werden durch Klicken auf **Benutzer wählt die Verzögerungszeitspanne aus** auf der Seite **Feedback und Timing** aktiviert.

- **Grenzen für die Verzögerung**
    - **Wie lange der Benutzer das Paket verzögern kann:** Wählen Sie aus, wie viele Stunden, Minuten oder Sekunden Pakete verzögert werden, wenn Benutzer im Verzögerungsdialogfeld auf **Warten** klicken.
    - **Benutzerverzögerung ist limitiert:** Legt fest, wie oft der Benutzer maximal auf **Warten** klicken darf, wenn das Verzögerungsdialogfeld angezeigt wird.
    - **Wie oft der Benutzer verzögern darf:** Das Verzögerungslimit.

- **Verhalten bei abgemeldetem Benutzer**
  - **Installation fortsetzen** Dies ist die Standardeinstellung. Setzt die Installation fort, wenn Benutzer abgemeldet ist.

    Beachten Sie, dass die auf der Seite **Konten** der Paketeigenschaften definierten Kontoeinstellungen für die Paketinstallation die Optionen für das Verhalten bei abgemeldetem Benutzer in einer Verteilungsmethode überschreiben.

    Wenn Sie in den Paketeigenschaften festlegen, die Installation als aktueller Benutzer durchzuführen und als Verteilungsmethode für abgemeldete Benutzer **Installation fortsetzen** auswählen, erzeugt dies einen Konflikt, der dazu führt, dass die Paketinstallation auf allen Geräten fehlschlägt, bei denen der aktuellen Benutzer nicht angemeldet ist.
  - **Installation fehlschlagen lassen:** Lässt die Installation fehlschlagen, wenn der Benutzer abgemeldet ist, unabhängig davon, welche Kontoeinstellungen in den Paketeigenschaften vorliegen.
- **Benutzerverhalten und Timeoutoptionen**
  - **Erst nach Erhalt der Benutzerantwort fortsetzen:** Das Verzögerungsdialogfeld wird angezeigt und wartet eine Benutzerantwort ab, unabhängig davon, welche Verzögerungszeit Sie angegeben haben. Wenn Benutzer zu lange mit der Antwort auf sich warten lassen oder niemand am Computer sitzt, kann der Task aufgrund eines Timeouts fehlschlagen..

    Wenn Benutzerfeedback erwartet wird, können Sie aus einer Liste die auszuführende Standardaktion auswählen. Klicken Sie auf die Optionsschaltfläche neben der Liste und wählen Sie **Abbrechen**, **Paket ausführen** oder **Verzögern** aus. Anschließend können Sie dann eingeben, wie lange das Verzögerungsdialogfeld auf eine Antwort wartet, bevor die von Ihnen ausgewählte Aktion ausgeführt wird.
  - **Zeitraum bis zur obengenannten Aktion:** Die Zeitspanne, die verstreicht, bevor die Aktion aus der Dropdownliste ausgeführt wird.

Informationen zur Seite "Benutzerdefinierte Nachricht" (unter der Seite "Feedback und Timing")

Diese Seite verwenden Sie, wenn Sie eine Nachricht für das Verzögerungsdialogfeld definieren möchten. Dieses Dialogfeld wird nur angezeigt, wenn Sie Verzögerungen zulassen. Die HTML-Seitenquelle für die Verzögerungsseiten befindet sich auf dem Coreserver im Ordner LDLogon\html\.

- **Benutzerdefinierte HTML-Startseiten verwenden:** Verwendet die HTML-Seiten im Ordner LDLogon\html\ des Coreservers.
- **Eine benutzerdefinierte Nachricht in das Verzögerungsdialogfeld aufnehmen:** Fügt dem Verzögerungsdialogfeld Text hinzu, den Sie eingeben (einschließlich HTML-Formatierung); hierbei wird der normalerweise eingefügte Standardtext überschrieben. Im Dialogfeld können weiterhin die Schaltflächen **Warten**, **Abbrechen** und **Jetzt installieren** zusammen mit der Beschreibung ihrer Funktionsweise angezeigt werden.

Die Seite "Richtlinienfrequenz und -typ"

Diese Seite wird für richtlinienbasierte Verteilungsmethoden angezeigt und beeinflusst das Verhalten der Zielgeräte beim Empfang der Richtlinie.

- **Erforderlich:** Der richtlinienbasierte Verteilungsagent wendet die erforderlichen Richtlinien an, ohne dass eine Eingabe seitens der Benutzer erforderlich ist. Sie können festlegen, dass erforderliche Richtlinien im Hintergrund ausgeführt werden. Benutzeroberflächen, die während der Installation eines

erforderlichen Tasks auf dem Gerät angezeigt werden, dürfen keine Abläufe blockieren. Das heißt, für die Installation der Anwendung darf keine Eingabe seitens des Benutzers erforderlich sein.

- **Empfohlen:** Benutzer können selbst entscheiden, wann empfohlene Richtlinien installiert werden. Empfohlene Richtlinien werden standardmäßig auf der Benutzeroberfläche des Geräts ausgewählt.
- **Optional:** Benutzer können selbst entscheiden, wann optionale Richtlinien installiert werden. Optionale Richtlinien werden nicht standardmäßig auf der Benutzeroberfläche des Geräts ausgewählt.

Sie können auch konfigurieren, wie häufig eine Richtlinie ausgeführt werden kann.

- **Einmal:** Sobald eine Richtlinie erfolgreich auf einem Gerät ausgeführt wurde, wird sie von dem betreffenden Gerät nicht mehr ausgeführt.
- **Wie gewünscht:** Das Paket kann jederzeit vom Benutzer installiert werden.
- **Periodisch:** Wenn eine empfohlene oder optionale Richtlinie als periodisch definiert wird, wird sie von der Benutzeroberfläche entfernt, sobald sie erfolgreich verarbeitet wurde. Sie wird wieder auf der Benutzeroberfläche angezeigt, nachdem das angegebene Intervall abgelaufen ist.

Informationen zur Seite "Offline"

Auf dieser Seite konfigurieren Sie, was geschieht, wenn ein Gerät zur Installation eines Pakets bereit ist, das Gerät jedoch keine Verbindung zum Coreserver herstellen kann. Dieser Fall kann eintreten, wenn sich die Dateien eines Pakets im lokalen Verteilungscache eines Geräts befinden und ein Benutzer, der unterwegs ist oder keine Netzwerkverbindung hat, versucht, dieses Paket zu installieren.

- **Warten, bis das Gerät den Kontakt zum verwalteten Coreserver herstellen kann:** Die Installation wird nur zugelassen, wenn das Gerät die Integrität der im Verteilungscache befindlichen Paketdatei beim Coreserver verifizieren kann. Die sicherste Option.
- **Paket(e) offline installieren:** Das Paket kann auf der Basis der im Verteilungscache vorhandenen Dateien installiert werden, ohne dass eine Verbindung zum Coreserver hergestellt werden muss.

Die Seite "Downgraden"

Diese Seite verwenden Sie zum Konfigurieren des Verteilungsverhaltens, wenn entweder das Zielbetriebssystem oder die Agenten des Zielgeräts die von Ihnen ausgewählten Verteilungsmethoden nicht unterstützen. Beispiel: Wenn es auf Ihren Geräten ältere Management Suite-Agenten gibt, unterstützen diese vielleicht kein Multicast- oder Peer-Download.

Downgradeoptionen für das Betriebssystem:

- **Funktionalität auf die Ebene des Betriebssystems downgraden:** Diese Option lässt zu, dass Tasks weiter ausgeführt werden, obwohl vielleicht nicht alle Optionen, die Sie für die Verteilungsmethode ausgewählt haben, aktiviert sind.
- **Fehler, falls das Betriebssystem die Standardfunktionalität nicht unterstützt:** Der Task schlägt fehl, wenn das Betriebssystem nicht die von Ihnen für die Verteilungsmethode ausgewählten Optionen unterstützt.

Downgradeoptionen für das Gerät:

- **Funktionalität auf die Ebene des Agenten downgraden:** Diese Option lässt zu, dass der Task weiter ausgeführt wird, obwohl vielleicht nicht alle Optionen, die Sie für die Verteilungsmethode ausgewählt haben, aktiviert sind.
- **Fehler, wenn der Agent die Standardfunktionalität nicht unterstützt:** Der Task schlägt fehl, wenn die Agenten die von Ihnen für die Verteilungsmethode ausgewählten Optionen nicht unterstützen.

Informationen zur Seite "Erkennung"

Mit dieser Seite können Sie Optionen für die Geräteerkennung auswählen. Damit der "Geplanter Task"-Handler einen Job verarbeiten kann, muss er die aktuelle IP-Adresse des Geräts ausfindig machen. Mit dieser Registerkarte können Sie festlegen, wie der Dienst mit den Geräten Kontakt aufnimmt.

Erkennungsoptionen:

- **UDP:** Wenn Sie UDP auswählen, wird ein Ping Discovery Service (PDS)-Ping über UDP verwendet. Die meistenManagement Suite-Gerätebestandteile setzen PDS voraus. Aus diesem Grund sollte auf Ihren verwalteten Geräten PDS installiert sein. PDS ist Teil des Standard LANDesk Agent. Dies ist die schnellste Erkennungsmethode und gleichzeitig der Standard. Mit UDP können Sie auch die UDP-Ping-Wiederholungen und das Timeout bestimmen.
- **TCP:** Wenn Sie TCP auswählen, wird eine HTTP-Verbindung mit dem Server auf Port 9595 benutzt. Diese Erkennungsmethode hat den Vorteil, dass sie über eine Firewall hinweg einsatzfähig ist, wenn Sie Port 9595 öffnen; die Methode unterliegt jedoch HTTP-Verbindungs-Timeouts, wenn keine Geräte vorhanden sind. Diese Timeouts können 20 Sekunden oder länger beanspruchen. Wenn eine große Zahl von Zielgeräten nicht auf die TCP-Verbindung reagiert, dauert es einige Zeit, bis Ihr Task gestartet werden kann.
- **Beide:** Wenn Sie "Beide" auswählen, versucht der Dienst die Erkennung erst mit UDP, dann mit TCP und zuletzt mit DNS/WINS (sofern ausgewählt) durchzuführen.
- **Anzahl Wiederholungen:** Wie viele Erkennungsversuche unternommen werden sollen.
- **Timeout für die Erkennung:** Wie lange bei jedem Erkennungsversuch auf eine Reaktion gewartet werden soll.
- **Timeout für Subnetzbroadcasts:** Wie lange auf eine Antwort für Subnetz-Broadcasts gewartet werden soll.
- **Subnetz-Broadcast deaktivieren:** Deaktiviert die Erkennung über ein Subnetz-Broadcast. Wenn ausgewählt, veranlasst diese Option die Weiterleitung eines Subnetz-gesteuerten Broadcast über UDP unter Verwendung von PDS.
- **DNS/WINS-Lookup deaktivieren:** Deaktiviert einen Name Service Lookup für jedes Gerät, wenn die ausgewählte TCP/UDP-Erkennungsmethode scheitert.

Das Statusfenster "Multicast Software Distribution"

Dieses Fenster wird auf dem Core angezeigt, wenn eine aktive Verteilung über Targeted Multicast durchgeführt wird. In diesem Fenster werden die folgenden Informationen angezeigt:

- **Paket-URL oder UNC-Pfad:** Dies ist der Speicherort des Pakets, das Sie gegenwärtig verteilen möchten. Diese Zeile wird mit der aktuellen Datei aktualisiert, die gegenwärtig übertragen wird.
- **Status:** Ein Echtzeitbericht über das Fortschreiten der Verteilung bzw. über den Erfolg des abgeschlossenen Tasks.
- **Multicastdomänen:** Das Feld oben zeigt alle Subnetze und die Multicast-Domänenrepräsentanten, die bei der Verteilung verwendet werden. Wenn Sie jeden Domänenrepräsentanten markieren, zeigt das untere Fenster alle Computer an, die ihre Verteilung von diesem Domänenrepräsentanten erhalten. Jeder Computer im unteren Fenster zeigt Informationen über den Abschluss der Verteilung auf diesem Computer an. Es gibt mehrere Informationsfelder auf der rechten Seite der aufgeführten Computer, einschließlich Felder über nicht erhaltene Pakete, Anforderungen für erneutes Senden und zum Verlangsamen. Diese Felder enthalten erst Informationen, wenn die Verteilung abgeschlossen ist.
- **Nicht erhaltene Pakete:** Zeigt an, wie viele Pakete das Gerät nicht vom Subnetzrepräsentanten beziehen konnte. Wenn die Zahl ungleich 0 war, ist die Verteilung misslungen.

- **Anforderungen erneut senden:** Zeigt an, wie oft das Gerät ein erneutes Senden dieses Paket vom Subnetzrepräsentanten anfordern musste. Dies ist eine gute Methode, um abzuschätzen, wie beschäftigt das Gerät mit der Handhabung von anderen Vorgängen während der Verteilung war.
- **Anforderungen verlangsamen:** Zeigt an, wie oft das Gerät eine Verlangsamung des Paketstroms anfordern musste. In diesem Fall zeigen hohe Zahlen in der Regel an, dass beim Computer Hardwareprobleme vorliegen, die die Verteilung verlangsamen. Wenn Sie viele Computer mit Anforderungen zum Verlangsamen haben, sollten Sie die Verzögerungs-/Paketnummer auf dem Subnetzrepräsentanten prüfen. Häufig liegt ein Zusammenhang zwischen der Verzögerungs-/Paketnummer und der Zahl der Anforderungen nach einem Verlangsamen vor.

Das Fenster wird automatisch nach 10 Sekunden geschlossen. Wenn das Fenster während der gesamten Verteilung geöffnet bleiben soll, klicken Sie auf **Dialogfeld geöffnet lassen**. Das Fenster bleibt geöffnet, bis Sie es manuell schließen. Wenn dieses Dialogfeld geöffnet bleibt, wird die Skriptausführung beendet. Daher müssen Sie darauf achten, dass Sie das Dialogfeld schließen.

Erstellen von benutzerdefinierten Skripten

Wenn Sie ein benutzerdefiniertes Skript aus einer Vorlage erstellen möchten, können Sie die Option **Benutzerdefiniertes Skript erstellen** verwenden.

So erstellen Sie ein benutzerdefiniertes Skript

1. Klicken Sie auf **Extras > Verteilung > Skripte verwalten**.
2. Klicken Sie im Kontextmenü **Alle anderen Skripte** auf **Benutzerdefiniertes Skript erstellen**.
3. Passen Sie das Skript an. Wenn Sie das Skript im Editor öffnen wollen, der mit dem Dateityp ".INI" verknüpft ist, klicken Sie auf **Editor verwenden**. Stellen Sie sicher, dass Sie die Datei speichern, bevor Sie den Editor schließen, wenn Sie damit die Datei bearbeitet haben.
4. Geben Sie einen **Namen für das benutzerdefinierte Skript** ein. Klicken Sie auf **OK**.

Erstellen von Dateibereitstellungsskripten

Wenn Sie nur Dateien auf Geräte kopieren möchten, können Sie ein Dateibereitstellungsskript verwenden. Sie können jeden Dateityp, einschließlich Textdateien, in ein angegebenes Verzeichnis auf dem Gerät übertragen. Dateibereitstellungsskripte unterstützen Targeted Multicast.

So verteilen Sie Dateien

1. Klicken Sie auf **Extras > Verteilung > Skripte verwalten**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neues Dateiübertragungsskript**.
3. Geben Sie einen **Skriptnamen** und ein **Zielverzeichnis** ein. Klicken Sie auf **Weiter**.
4. Wählen Sie auf den folgenden drei Seiten die Bandbreite, den Task und die Multicastoptionen aus, die Sie verwenden möchten.
5. Wählen Sie auf der Seite **Bereitzustellende Dateien auswählen** Dateien aus, indem Sie einen **Webpfad** oder **Dateifreigabepad** auswählen. Geben Sie den Pfad ein, und fügen Sie der Liste die gewünschten Dateien hinzu. Klicken Sie auf **Weiter**.
6. Lesen Sie die Zusammenfassung auf der Seite **Fertig**, und klicken Sie auf **Fertigstellen**.

Die folgenden Abschnitte beschreiben die Seiten und Optionen im Assistenten **Dateibereitstellungsskript erstellen**.

Die Seite "Allgemeine Informationen"

Diese Seite verwenden Sie zum Konfigurieren allgemeiner Informationen zum Dateiübertragungsskript.

- **Skriptname:** Der Dateiname des Skripts. Die Dateinamenerweiterung ist standardmäßig .INI. Skripte werden im Ordner \Programme (x86)\LANDesk\ManagementSuite\scripts gespeichert.
- **Beschreibung:** Die Skriptbeschreibung, die im Extra "Skripte verwalten" erscheint.
- **Zielverzeichnis:** Das Verzeichnis auf den Clients, das die bereitgestellte Dateien aufnehmen wird.
- **Dateien mit Multicast verteilen:** Wählen Sie diese Option, wenn Sie Multicast verwenden möchten. Bei der Auswahl dieser Option werden die Seiten zu Multicastdomänen und Multicastlimits aktiviert.

Informationen zur Seite "Downloadoptionen"

Auf dieser Seite konfigurieren Sie die Bandbreitendrosselung und Paketverzögerungen.

- **Peer-Download (nur vom Cache oder Peer installieren):** Lässt einen Download von Paketen nur dann zu, wenn sie sich im lokalen Cache oder auf einem Peer in der gleichen Multicast-Domäne befinden. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Paketinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sich das Paket im lokalen Cache oder im Cache eines Peer befindet. Eine Möglichkeit zur Nutzung dieser Option besteht darin, das Paket zuerst mit der zuvor im Assistenten angezeigten Option **Nur Dateien auf dem Computer cachen, die Multicast verwenden** in jedem Subnetz auf ein Gerät zu kopieren.
- **Dynamische Bandbreitendrosselung:** Legt fest, dass der von einem Gerät erzeugte Netzwerkverkehr Vorrang vor dem durch die Verteilung bedingten Verkehr hat. Wenn Sie diese Option auswählen und den **minimal verfügbaren Bandbreitenprozentsatz** von 0 beibehalten, wird die Verteilung auf etwa ein Paket pro Sekunde gedrosselt, sobald das Gerät Netzwerkverkehr initiiert, und bleibt auf diesem Niveau, bis der Netzwerkverkehr endet. Diese Option erzwingt eine vollständigen Download der Datei in den Cache des Geräts. Damit wird gleichzeitig die Option für Checkpoint-Neustarts auf Byteebene aktiviert, sodass Downloadvorgänge im Fall einer Unterbrechung an der Stelle wieder aufgenommen werden, an der sie unterbrochen wurden. Wenn Sie ein ESWD- oder MSI-Paket erneut installieren oder reparieren, sollten Sie die Option **Dynamische Bandbreitendrosselung** nicht verwenden, weil bei diesen Pakettypen normalerweise nur die benötigten Dateien heruntergeladen werden.
- **Auf Client zu verwendender minimal verfügbarer Bandbreitenprozentsatz:** Legt den Umfang der dynamischen Bandbreitendrosselung fest. Sie können Werte bis zu 50 Prozent der für ein Gerät verfügbaren Gesamtnetzwerkbandbreite angeben. Wenn beispielsweise während der Verteilung eine andere Anwendung auf dem Gerät Netzwerkbrandbreite konsumiert und Sie den Brandbreitenprozentsatz mit 50 Prozent angeben, erhält der Verteilungstask 50 Prozent und die Geräteanwendung ebenfalls 50 Prozent. In der Praxis ist diese Prozentangabe variabel, weil das Betriebssystem je nach Anzahl und Priorität der Anwendungen, die Bandbreite benötigen, automatisch einen Großteil der Netzwerkbandbreite zuweist.
- **Verzögerung zwischen Paketen (Peer):** Diese Option legt die Verzögerung zwischen Paketen fest, die an Peers im gleichen Subnetz gesendet werden. Sie können Verteilungen mithilfe dieser Verzögerung beschleunigen und verlangsamen. Wenn die Verzögerung zwischen Paketen erhöht wird, erfolgt die Verteilung langsamer und unter geringerem Einsatz von Bandbreite. Sie können diese Option zusammen mit der Option **Dynamische Bandbreitendrosselung** verwenden. Wenn Sie dies tun, fällt die Paketverzögerung jedoch stärker ins Gewicht.
- **Verzögerung zwischen Paketen (Quelle):** Legt die Verzögerung zwischen der Paketquelle und dem Zielgerät fest. Wenn die Verzögerung zwischen Paketen erhöht wird, erfolgt die Verteilung langsamer und unter geringerem Einsatz von Bandbreite. Sie können diese Option zusammen mit der Option **Dynamische Bandbreitendrosselung** verwenden. Wenn Sie dies tun, fällt die Paketverzögerung jedoch stärker ins Gewicht.

Informationen zur Seite "Taskoptionen"

Auf dieser Seite konfigurieren Sie, wie die betreffende Verteilung bereitgestellt wird. Wenn Sie eine MSI-Datei oder eine generische ausführbare Datei verteilen, haben Sie die Option, beliebige Befehlszeilenparameter einzugeben, die nach dem Multicast an die Datei weitergegeben werden müssen.

- **Skript verwendet Standard-Distributionslimit:** Sie können die Zahl der Computer begrenzen, auf die Targeted Multicast die gleichzeitige Verteilung vornimmt. Diese Option verwendet den Standardwert, den Sie auf der Registerkarte **Konfigurieren > Dienste > Benutzerdefinierte Tasks** unter **Verteilen an X Computer gleichzeitig** festgelegt haben.
- **Skript verwendet benutzerdefiniertes Distributionslimit:** Verwenden Sie diese Option, um den Standard für den aktuellen Task durch Festlegen eines anderen Werts zu überschreiben.
- **Nur vom Cache oder Peer installieren:** Durch diese Option werden Zielcomputer daran gehindert, ihr Subnetz für die Installation eines Pakets zu überschreiten. Computer suchen zuerst in ihrem Multicast-Cacheverzeichnis. Wenn das Paket dort nicht vorhanden ist, führen sie die Prüfung auf Pakete mit Peers auf ihrem Subnetz durch. Wenn keiner der Peers das Paket besitzt, schlägt die Verteilung fehl. Diese Option minimiert den Netzwerkverkehr innerhalb von Subnetzen. Sie können diese Option verwenden, nachdem Sie ein Paket auf jedes Subnetz über die Seite "Skript erstellen" mit der Option **Nur Dateien auf dem Computer cachen, die Multicast verwenden** kopiert haben.
- **Datei vor Clientinstallation überprüfen:** Erzeugt eine Prüfsumme (CRC) für das zu verteilende Paket, sobald der Assistent beendet wird. Geräte können mithilfe dieses Prüfsummenwerts sicherstellen, dass die empfangene Datei/das Paket nicht beschädigt ist. Abhängig von der Größe der zu verteilenden Datei bzw. des Pakets, kann die Berechnung der Prüfsumme einige Minuten in Anspruch nehmen.
- **Versuchen Sie nicht "Task Completion" auszuführen:** Verwenden Sie diese Option, um zu verhindern, dass die Funktion "Task Completion" verwendet wird, um fehlgeschlagene Tasks erneut auszuführen. Wenn "Task Completion" auf einem Gerät installiert ist, versucht das System, fehlgeschlagene Tasks bei der nächsten Ausführung von "Task Completion" erneut auszuführen. Fehlgeschlagene Tasks werden dennoch protokolliert, wenn Sie diese Option verwenden.

Informationen zur Seite "Multicast-Domänenoptionen"

Diese Seite wird nur angezeigt, wenn Sie "Multicast" als Verteilungstyp ausgewählt haben. Auf dieser Seite konfigurieren Sie Multicast-Optionen.

- **Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Task durchzuführen. Bei dieser Option werden die Domänenerkennungsergebnisse für die erneute Verwendung nicht gespeichert.
- **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Verwenden Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Task durchzuführen und die Ergebnisse für eine künftige Verwendung zu speichern; somit sparen Sie Zeit bei folgenden Multicasts
- **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option immer dann, wenn Sie durch Targeted Multicast eine Domänenerkennung durchgeführt haben und speichern Sie die Ergebnisse.
- **Domänenrepräsentanten reaktivieren Computer:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan"-Technologie unterstützen, beim Empfang von Multicast reaktivieren möchten. Mit dem Dialogfeld **Multicast-Optionen** können Sie festlegen, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das "Wake on Lan"-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden.

- **Erweiterte Multicast-Optionen:** Verwenden Sie diese Option, um erweiterte Optionen festzulegen. Die Standardeinstellungen sind für die meisten Tasks geeignet.

Informationen zur Domänenerkennung

Die Domänenerkennung ist nur auf Netzwerken mit Subnetzen erforderlich, die gegenseitig ihren Multicast-Datenverkehr erkennen können. Wenn Ihre Subnetze den gegenseitigen Datenverkehr nicht erkennen, können Sie Zeit sparen, indem Sie zuerst die Ergebnisse einer Domänenerkennung speichern und dann die Option **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** auswählen; Targeted Multicast muss dann nicht vor jedem Task eine Domänenerkennung durchführen.

Erkennen Ihre Netzwerksubnetze den gegenseitigen Multicast-Datenverkehr jedoch, so können Sie die Leistung von Targeted Multicast beschleunigen, indem Sie die Domänen vorab mithilfe des Skripts multicast_domain_discovery.ini identifizieren, das sich im Verzeichnis ...\ManagementSuite\scripts befindet. Dieses Skript führt auf Zielcomputern keine Vorgänge aus. Führen Sie dieses Skript im Fenster **Geplante Tasks** für eine Liste mit Zielen aus, die Ihr gesamtes Netzwerk umspannt. Die Domänenerkennungsergebnisse werden dadurch für die künftige Verwendung gespeichert. Sie können dieses Skript regelmäßig vor großvolumigen Multicast-Verteilungen ausführen.

Wenn Sie **Cachedatei verwenden** unter **Konfigurieren > Management Suite Dienste > Multicast** ausgewählt haben, durchläuft Targeted Multicast einen Erkennungsvorgang, auch wenn Sie **Ergebnisse der letzten Multicast-Domänenerkennung verwenden** ausgewählt haben. Targeted Multicast muss dies durchführen, um herauszufinden, welche potenziellen Multicast-Domänenrepräsentanten die Datei in ihrem Cache gespeichert haben.

Informationen zum Dialogfeld "Multicastoptionen"

Mit dem Dialogfeld **Multicast-Optionen** des Dateibereitstellungsskript-Assistenten können Sie taskspezifische Targeted Multicast-Parameter konfigurieren. Die Standardwerte in diesem Dialogfeld sind in der Regel für die meisten Multicasts geeignet.

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Die Zahl der Repräsentanten, die aktiv zur selben Zeit einen Multicast durchführen, ist auf diese Anzahl beschränkt.
- **Verarbeitung von Rechnern einschränken, bei denen Multicast fehlschlug ...:** Wenn ein Gerät die Datei über Multicast nicht erhält, lädt es die Datei aus dem Web oder vom Dateiserver herunter. Dieser Parameter kann verwendet werden, um die Anzahl der Geräte zu beschränken, die die Datei gleichzeitig erhalten. Wenn z. B. die Höchstanzahl von Threads 200 war und die Höchstanzahl der fehlgeschlagenen Multicast-Threads bei 20 lag, würden im Dialogfeld **Benutzerdefinierte Tasks** nicht mehr als 20 Computer gleichzeitig verarbeitet werden, bei denen Multicast fehlgeschlagen ist. Das Dialogfeld **Benutzerdefinierte Tasks** verarbeitet bis zu 200 Geräte gleichzeitig, wenn diese erfolgreich den Multicast erhalten haben. Es verarbeiten jedoch nur maximal 20 der 200 Threads Geräte, bei denen der Multicast-Task misslungen ist. Wenn dieser Wert auf 0 festgelegt ist, führt das Dialogfeld **Benutzerdefinierte Tasks** den Verteilungsabschnitt des Task für keinen der Computer durch, auf dem das Multicasting fehlgeschlagen ist.
- **Anzahl von Tagen, die die Dateien im Cache des Clients verbleiben:** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache des jeweiligen Zielcomputers gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Anzahl von Tagen, die die Dateien im Cache des Multicast-Domänenrepräsentanten verbleiben:** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache auf dem Multicast-Domänenrepräsentanten gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.

- **Minimale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Mindestwartezeit zwischen dem Senden von Multicast-Paketen. Dieser Wert wird nur verwendet, wenn der Repräsentant kein Multicasting einer Datei aus dem eigenen Cache durchführt. Wenn dieser Parameter nicht festgelegt wird, wird die auf dem Subnetz/Domänenrepräsentantencomputer gespeicherte Mindestruhezeit verwendet. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.
- **Maximale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Höchstwartezeit zwischen dem Senden von Multicast-Paketen. Weitere Informationen finden Sie weiter oben unter "Mindestzahl in Millisekunden zwischen Paketübertragungen".
- **Wartezeit in Sekunden nach Wake on LAN:** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Informationen zur Seite "Bereitzustellende Dateien auswählen"

Die Seite **Bereitzustellende Dateien auswählen** wird im Dateiübertragungsskript-Assistenten angezeigt.

- **Webpfad:** Klicken Sie, um auf einem Webserver gespeicherte Pakete anzuzeigen. Sie müssen http:// in die URL-Angabe mit einschließen.
- **Dateifreigabepfad:** Klicken Sie, um Pakete in einer NULL-Sitzungsfreigabe auf dem Dateiserver anzuzeigen. Dieser Pfad muss den UNC-Pfadkonventionen \\servername\freigabename\ entsprechen.
- **Durchsuchen:** Klicken Sie auf **Durchsuchen**, um nach dem Pfad zu suchen. Wenn Sie auf **Webpfad** geklickt haben, wird ein kleines Fenster zum Durchsuchen angezeigt. Wenn Sie auf **Dateifreigabepfad** geklickt haben, wird ein Standarddialogfeld zum Durchsuchen angezeigt. Wenn Sie im Browserfenster "Paketspeicherort auswählen" ein Webserververzeichnis durchsuchen möchten, müssen Sie die URL mit einem nachgestellten Schrägstrich (/) angeben, da das Browserfenster sonst einen Fehler anzeigt.
- **Hinzufügen:** Verwenden Sie **Hinzufügen**, um ein Programm direkt aus dem Pfadbearbeitungsfeld hinzuzufügen, nachdem Sie den vollständigen Pfad und den Dateinamen eingegeben haben.
- **Entfernen:** Wählen Sie eine Datei aus, die Sie hinzugefügt haben und klicken Sie auf **Entfernen**, um eine Datei aus der Liste zu entfernen.

Informationen zur Seite "Fertig"

Diese Seite fasst die Aktionen zusammen, die Sie für die Installation des Pakets ausgewählt haben. Vergewissern Sie sich vor dem Fortsetzen des Vorgangs, dass die verwalteten Geräte alle Voraussetzungen erfüllen, die im Warnabschnitt aufgeführt sind.

Wenn Sie auf **Als Standard festlegen** klicken, werden die ausgewählten Konfigurationsoptionen als Standardwerte für diesen Assistenten festgelegt.

Klicken Sie auf **Fertig**, um dann einen Zeitplan für die Skriptverteilung zu erstellen.

Verwaltung von Anwendungsrichtlinien (Application Policy Management)

Informationen zur richtlinienbasierten Verwaltung

Mit der richtlinienbasierten Verwaltung können Anwendungsgruppen problemlos auf mehreren Geräten verwaltet werden. Wie jeder andere geplante Task benötigen auch die Richtlinien Folgendes:

- Ein SWD-Paket, MSI, Programmdatei, Batchdatei oder ein von Ihnen erstelltes Macintosh-Paket.
- Eine Verteilungsmethode, die Richtlinien unterstützt, entweder richtlinienbasiert oder richtlinienbasierter Push.
- Richtlinienziele für die Verteilungspakete, z. B. die Ergebnisse einer LDAP- oder Coredatenbankabfrage
- Ein geplanter Zeitpunkt, zu dem die Richtlinie zur Verfügung gestellt werden sollte.

Die richtlinienbasierte Verwaltung wiederholt in regelmäßigen Abständen die Ausführung von Abfragen, die Sie als Teil der Richtlinie definiert haben. Auf diese Weise werden Ihre Richtlinien auf alle neu hinzukommenden verwalteten Geräte angewendet. Angenommen im LDAP-Verzeichnis gibt es einen Container "Abteilung", der Benutzerobjekte enthält. Alle Benutzer, deren Abteilungsobjekt "Marketing" ist, verwenden die Standardanwendungen. Nachdem Sie eine Richtlinie für die "Marketing"-Benutzer eingerichtet haben, werden auf den Computern der Benutzer, die dem Objekt "Marketing" neu hinzugefügt werden, automatisch die richtigen Anwendungen installiert.

Mit der -Konsole können Sie Anwendungsrichtlinien konfigurieren, die in der Coredatenbank gespeichert sind.

Die richtlinienbasierte Verwaltung kann folgende Dateitypen bereitstellen:

- MSI
- Ausführbare Datei
- Batchdatei
- Macintosh
- Linux-RPM
- LANDesk Application Virtualization
- Windows Script Host Package (.wsf)
- Legacy-SWD-Paket

Der Taskablauf für die richtlinienbasierte Verwaltung sieht folgendermaßen aus:

1. Stellen Sie sicher, dass die Softwareverteilungsagenten auf Ihren Geräten installiert sind.
2. Falls für die Anwendung, für die Sie eine Richtlinie verwenden möchten, kein Paket vorhanden ist, müssen Sie eines erstellen. Weitere Informationen finden Sie unter "Softwareverteilung/Verteilungspakete/Verteilungsmethoden" auf Seite 269.
3. Verwenden Sie das Fenster "Verteilungspakete", um eine Paketdefinition für das Paket zu erstellen.
4. Erstellen oder wählen Sie eine vorhandene richtlinienbasierte Verteilungsmethode aus.
5. Erstellen Sie einen Softwareverteilungstask im Fenster **Geplante Tasks** und wählen Sie das Paket und die Verteilungsmethode aus, das/die Sie weiter oben erstellt haben.

6. Wählen Sie die Ziele für die Richtlinie aus. Diese Auswahl kann jede Kombination aus individuellen Geräten, Datenbankabfragen, Gerätegruppen, LDAP-Elementen und LDAP-Abfragen einschließen.
7. Legen Sie einen Ausführungszeitpunkt für den Task fest. Bei seiner Ausführung wird das Verteilungspaket für einen Pull-Vorgang zur Verfügung gestellt.
8. Der richtlinienbasierte Verwaltungsdienst auf dem Coreserver aktualisiert in regelmäßigen Abständen die Liste der Richtlinienziele durch eine Neubewertung der Ergebnisse von LDAP-/Datenbankabfragen. Hiermit wird sichergestellt, dass die Gruppe der Zielbenutzer/-computern in der Coredatenbank immer dem aktuellen Stand entspricht.
9. Ein Benutzer meldet sich bei einem Gerät an, stellt eine Verbindung zum Netzwerk her oder startet den Agent für die richtlinienbasierte Verwaltung auf andere Weise.
10. Der richtlinienbasierte Verwaltungsdienst des Coreservers ermittelt anhand der Geräte-ID des Geräts und des angemeldeten Benutzers oder des LDAP-Gerätestandorts die relevanten Richtlinien.
11. Der richtlinienbasierte Verwaltungsdienst sendet die Richtliniendaten zurück an den Agent der richtlinienbasierten Verwaltung.
12. Abhängig davon, wie Sie die Richtlinienverarbeitung auf dem Gerät konfiguriert haben, muss der Benutzer die auszuführenden Richtlinien auswählen oder die Richtlinien werden automatisch ausgeführt. In der Liste des Geräts stehen nur empfohlene oder optionale Richtlinien zur Verfügung. Noch nicht verarbeitete empfohlene Richtlinien werden in der Liste standardmäßig mit einem Häkchen gekennzeichnet. In regelmäßigen Abständen ausgeführte Richtlinien werden in der Liste angezeigt, sobald ihr Ausführungsintervall abgelaufen ist. Ausgewählte Richtlinien werden nacheinander ausgeführt.
13. Der Agent der richtlinienbasierten Verwaltung sendet die Richtlinienergebnisse an den Coreserver, der die Ergebnisse in der Coredatenbank speichert. Der Status der richtlinienbasierten Verwaltung wird an den Coreserver weitergeleitet; zur Verbesserung der Zuverlässigkeit wird hierbei HTTP verwendet. Der Status wird im Fenster "Geplante Tasks" angezeigt.

Konfigurieren von Richtlinien

Die richtlinienbasierte Verwaltung benötigt für alle Richtlinien, die Sie erstellen, einen unterstützten Verteilungspakettyp. Die Pakete können entweder vorab oder beim Erstellen der Richtlinie erstellt werden. Es wird empfohlen, die Pakete im Voraus zu erstellen, damit Sie sie testen können, bevor sie für eine Richtlinie verwendet werden.

Normale Verteilungen und Richtlinien können dasselbe Verteilungspaket verwenden. Der Unterschied liegt in der Bereitstellung, nicht in der Paketerstellung. Es gibt zwei Verteilungsmethoden, die die richtlinienbasierte Verteilung unterstützen:

- **Richtlinienverteilungsmethoden:** Verteilung als reines Richtlinienmodell. Nur Geräte, die die Richtlinienkriterien erfüllen, erhalten das Paket.
- **Richtlinienunterstützte Pushverteilungsmethoden:** Die kombinierte Pushverteilung und das Richtlinienmodell. Zuerst versucht die Softwareverteilung, das Paket auf allen Geräten in der Zielliste zu installieren. Auf diese Weise können Sie eine erstmalige Bereitstellung mittels Targeted Multicast durchführen. Im zweiten Schritt erhalten alle Geräte, auf denen das Paket nicht angekommen ist oder die erst später zur Zielliste hinzugefügt wurden (beispielsweise im Fall einer dynamischen Zielliste), das Paket, wenn der richtlinienbasierte Verwaltungsagent auf dem Gerät das Paket anfordert.

Der Hauptunterschied zwischen der Standardverteilungsmethode und der richtlinienbasierten Verteilung besteht darin, dass das Dialogfeld für richtlinienbasierte **Verteilungsmethoden** über eine Seite mit der Bezeichnung **Jobtyp und Häufigkeit** verfügt.

Die Jobtyp- und Häufigkeitsoptionen beeinflussen das Verhalten der Zielgeräte beim Empfang der Richtlinie:

- **Erforderlich:** Der Agent der richtlinienbasierten Verwaltung überträgt die erforderlichen Richtlinien, ohne dass eine Eingabe seitens des Benutzers erforderlich ist. Sie können festlegen, dass erforderliche Richtlinien im Hintergrund ausgeführt werden. Benutzeroberflächen, die während der Installation eines erforderlichen Tasks auf dem Gerät angezeigt werden, dürfen keine Abläufe blockieren. Das heißt, für die Installation der Anwendung darf keine Eingabe seitens des Benutzers erforderlich sein.
- **Empfohlen:** Benutzer können selbst entscheiden, wann empfohlene Richtlinien installiert werden. Empfohlene Richtlinien werden standardmäßig auf der Benutzeroberfläche des Geräts ausgewählt.
- **Optional:** Benutzer können selbst entscheiden, wann optionale Richtlinien installiert werden. Optionale Richtlinien werden nicht standardmäßig auf der Benutzeroberfläche des Geräts ausgewählt.

Sie können auch konfigurieren, wie häufig eine Richtlinie ausgeführt werden kann.

- **Einmal:** Sobald eine Richtlinie erfolgreich auf einem Gerät ausgeführt wurde, wird sie von dem betreffenden Gerät nicht mehr ausgeführt.
- **Periodisch:** Wenn eine empfohlene oder optionale Richtlinie als periodisch definiert wird, wird sie von der Benutzeroberfläche entfernt, sobald sie erfolgreich verarbeitet wurde. Sie wird wieder auf der Benutzeroberfläche angezeigt, nachdem das angegebene Intervall abgelaufen ist.
- **Wie gewünscht:** Kann jederzeit vom Benutzer installiert werden.

Erstellen einer richtlinienbasierten Verteilung

Richtlinienbasierte Verteilungen werden wirksam, sobald der Richtlinientask gestartet wird und die Ziele identifiziert wurden. Richtlinienbasierte Pushverteilungen werden ausgeführt, sobald die erste pushbasierte Verteilung abgeschlossen ist.

So erstellen Sie eine richtlinienbasierte Verteilung

1. Klicken Sie in der Konsole auf **Extras > Verteilung > Verteilungsmethoden**.
2. Klicken Sie mit der rechten Maustaste auf **Richtlinienbasierte Verteilung** oder **Richtlinienunterstützte Pushverteilung** und dann auf **Neue Verteilungsmethode**.
3. Konfigurieren Sie die Optionen für die Verteilungsmethode Ihren Vorstellungen entsprechend. Klicken Sie auf **Hilfe**, um weitere Informationen zu den einzelnen Seiten abzurufen.
4. Wählen Sie die gewünschten Optionen bzgl. **Richtlinienfrequenz und Typ** aus.
5. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben.
6. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
7. Klicken Sie in der Symbolleiste auf die Schaltfläche **Softwareverteilung**.
8. Konfigurieren Sie die gewünschten Taskoptionen und klicken Sie auf **OK**.
9. Wenn die richtlinienbasierte Verteilung ausgewählt ist, ziehen Sie die Richtlinienziele in den rechten Fensterausschnitt.

Hinzufügen von Richtlinienzielen

Beim Erstellen eines richtlinienbasierten Tasks ist es häufig sinnvoll, die Richtlinie zunächst nur auf einer kleinen Zielgruppe bereitzustellen. Sollten beim Bereitstellen der Richtlinie Probleme auftreten, so bleibt mit dieser Vorgehensweise der Schaden auf einen kleinen Benutzerkreis begrenzt. Nachdem die Ergebnisse der Bereitstellung in der kleinen Benutzergruppe validiert wurden, können Sie weitere Ziele zur Richtlinie hinzufügen. Wenn neue Ziele zu einem aktiven Richtlinientask hinzugefügt werden, steht die Richtlinie den neu als Ziel angesprochenen Geräten oder LDAP Objekten direkt zur Verfügung.

Hinzufügen statischer Ziele

Die richtlinienbasierte Verwaltung kann statische Ziele als Richtlinienziele verwenden. Statische Ziele sind in einer Liste geführte Geräte oder Benutzer, die ausschließlich manuell geändert werden können. Fügen Sie statistische Ziele hinzu, indem Sie einzelne Geräte aus der Netzwerkansicht als Ziele auswählen. Einzelne LDAP Geräte können nicht als statische Ziele hinzugefügt werden.

Hinzufügen dynamischer Ziele

Die richtlinienbasierte Verwaltung kann Richtlinienziele mithilfe von Abfragen ermitteln. Abfragen werden ausschließlich in der Coredatenbank gespeichert. Weitere Informationen zum Erstellen von Abfragen finden Sie unter "Abfragen/Verzeichnis-Manager" auf Seite 193.

Dynamische Ziele können Gerätegruppen in der Netzwerkansicht, LDAP Objekte, LDAP Abfragen und Inventarabfragen beinhalten.

Damit Geräte Richtlinien empfangen können, die über Active Directory als Ziele angesprochen werden, müssen die Geräte für die Anmeldung beim Verzeichnis konfiguriert sein. Das bedeutet, dass die richtige Agentensoftware installiert sein muss. Außerdem müssen sich die Agenten beim richtigen Verzeichnis anmelden, damit ihr eindeutiger, definierter Name dem Namen entspricht, der über den Verzeichnis-Manager und den Scheduled Tasks Application Policy Manager angegeben wurde.

Um ein Gerät von LDAP aus als Ziel anzusprechen, muss jedes Windows-Gerät über ein Computerkonto auf dem Active Directory-Domänencontroller verfügen. Das heißt, der als Gerät verwendete Computer muss bei der Domäne angemeldet sein, in der Active Directory gespeichert ist. Sie können nicht einfach ein Netzlaufwerk mit dem voll qualifizierten Windows-Domänennamen verbinden. Die Richtlinie wird in diesem Fall nicht angewendet.

So verwenden Sie den Verzeichnis-Manager zum Erstellen einer Abfrage

1. Klicken Sie auf **Extras > Verteilung > Verzeichnis-Manager**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Verzeichnis verwalten**.
3. Geben Sie den Verzeichnis-URL und die Authentifizierungsdaten ein und klicken Sie auf **OK**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Abfrage**.
5. Erstellen Sie die Abfrage. Weitere Informationen finden Sie unter "LDAP-Abfragen" auf Seite 195.

Wie sich Bereiche auf die Sichtbarkeit von Richtlinienzielen auswirken

Mehrere Bereiche können den Fensterausschnitt "Zieldetails" der richtlinienbasierten Verwaltung filtern, um eine Zielliste zu erhalten. Jedoch entspricht der von einer Richtlinie verwendete endgültige Bereich immer dem Bereich des Taskeigentümers.

Wenn der Richtlinientask unter **Globale Tasks** aufgeführt wird und ein anderer Management Suite-Benutzer, der über einen anderen Bereich verfügt, die Zieldetailanzeige für den Task anzeigt (diese zweite Person soll in diesem Fall ein "Ziellisteneditor" sein), wird die Zieldetailanzeige durch den Bereich des Editors gefiltert. In diesem Fall sieht der Editor möglicherweise nicht alle Ziele im Fensterausschnitt "Zieldetails", auf die die Richtlinie angewendet wird, da es ihm sein Bereich nicht erlaubt, alle Ziele im Bereich des Erstellers anzuzeigen.

Softwarebereitstellungsportal

Anwendungsrichtlinien werden immer mit einem Pull-Modell verarbeitet. Geräte überprüfen auf dem Coreserver, ob neue Richtlinien für sie vorhanden sind. Bei dieser Überprüfung wird auf dem Gerät ein Dialogfeld angezeigt, in dem nur unverarbeitete empfohlene und optionale Richtlinien angezeigt werden. Erforderliche Richtlinien werden nicht angezeigt. Eine noch nicht verarbeitete, empfohlene Richtlinie wird in der Benutzeroberfläche standardmäßig ausgewählt, um den Benutzer zu veranlassen, sie zu verarbeiten.

Nachdem eine Richtlinie verarbeitet wurde, wird sie unter Umständen weiterhin auf der Benutzeroberfläche angezeigt wird, wenn sie für die regelmäßige Ausführung vorgesehen ist. In diesem Fall bleibt sie ausgewählt, selbst wenn es sich um eine empfohlene Richtlinie handelt. Eine Richtlinie wird auch dann weiterhin auf der Benutzeroberfläche angezeigt, wenn sie nicht richtig angewendet wurde.

Der Softwareverteilungsagent auf verwalteten Geräten stellt auch ein Portal für die Softwarebereitstellung zur Verfügung. Das Portal überprüft den lokalen Cache der Softwareverteilung auf Richtlinien, die für das lokale Gerät/den lokalen Benutzer gelten. Anschließend listet das Portal eine Seite mit verfügbaren Richtlinien auf. Benutzer können eine Richtlinie aus der Liste auswählen und auf **Bereitstellen** klicken, um die mit der Richtlinie verknüpften Pakete zu installieren.

So öffnen Sie das Softwarebereitstellungsportal

1. Klicken Sie auf einem verwalteten Gerät auf **Start > Programme > LANDesk Management > Desktop Manager** und klicken Sie dann auf die Schaltfläche **Softwarebereitstellung**.
2. Wählen Sie die Richtlinie aus, die Sie anwenden möchten.
3. Klicken Sie auf **Bereitstellen**.

HINWEIS: Sie können die Liste der verfügbaren Richtlinien manuell aktualisieren, indem Sie auf der Seite **Softwarebereitstellung** auf die Schaltfläche **Aktualisieren** klicken.

Softwarelizenzüberwachung

Softwarelizenzüberwachung – Übersicht

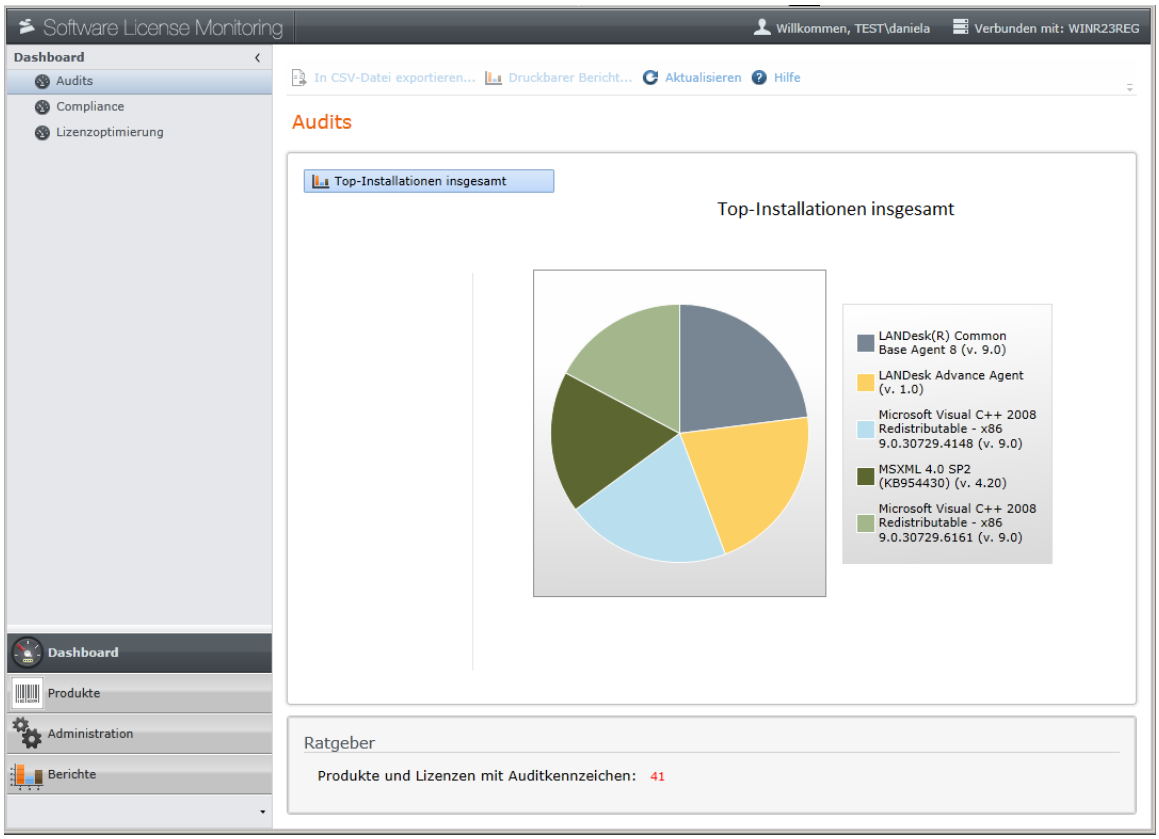
Die Softwarelizenzüberwachung (SLM, Software License Monitoring) gibt Ihnen Verwaltungstools zur Überwachung der Softwarenutzung und Lizenzcompliance und zur Kostenkontrolle in Ihrem Unternehmen an die Hand.

Für IT-Administratoren und Softwareassetmanager ist es oft nicht einfach, die Produkte zu verfolgen, die auf den zahlreichen Geräten innerhalb eines Netzwerks installiert sind. Sie laufen nicht nur Gefahr, eine größere Anzahl von Produkten zu installieren, als entsprechende Lizenzen erworben wurden, sondern sondern auch, zu viele Lizenzen zu kaufen. Sie können diese Probleme vermeiden, indem Sie mithilfe der SLM-Konsole den Einsatz von Produktlizenzen und die Verwendung von Produkten innerhalb Ihres Unternehmens überwachen und die betreffenden Daten in Berichten zusammenstellen.

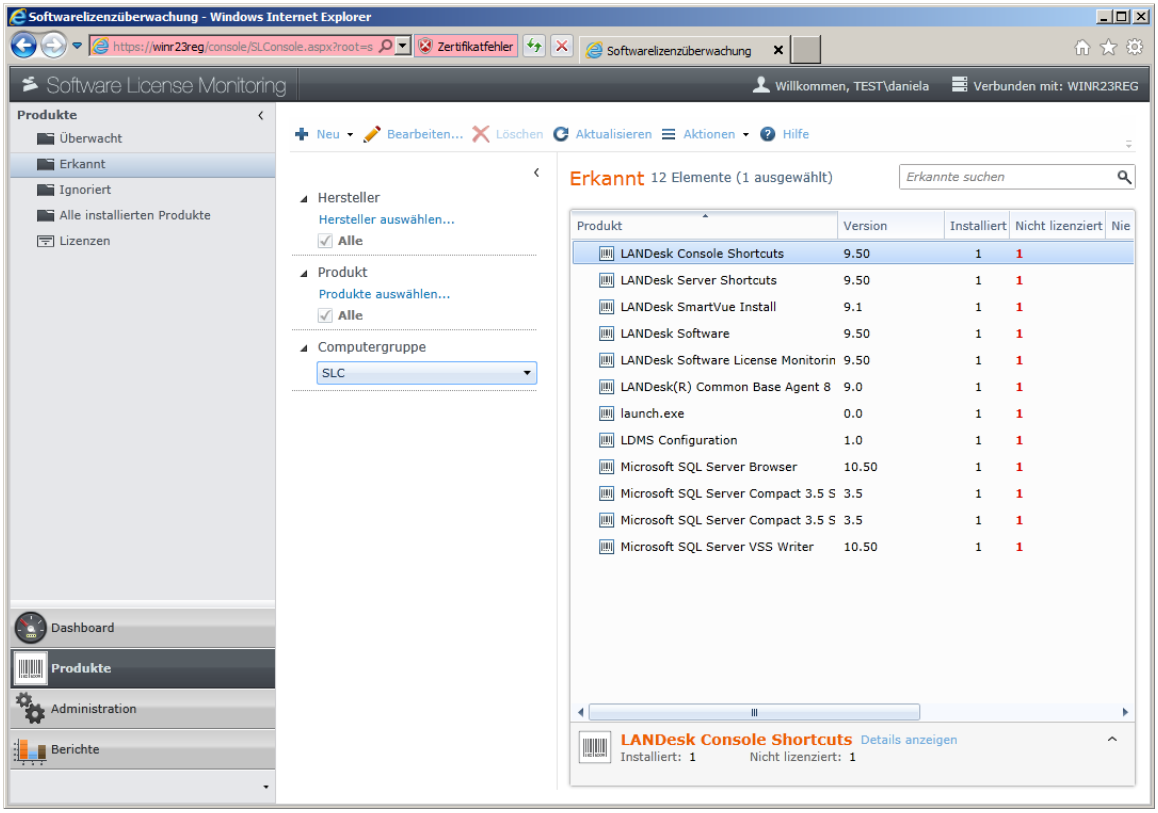
Die SLM-Konsole

Die Konsole für die Softwarelizenzüberwachung (SLM-Konsole) wird in einem Webbrowser geöffnet. Sie bietet zwei verschiedene Typen von Seiten für die Anzeige von Daten:

Seiten vom Typ **Dashboard** zeigen Übersichtsdiagramme zu wesentlichen Produkt- und Lizenzdaten an. Diese sind zur Planung von Audits und zur Optimierung der Lizenznutzung nützlich.



Seiten vom Typ **Produkte** zeigen detaillierte Daten zu den auf verwalteten Geräten installierten Produkten an. Diese Seiten enthalten Lizenzdaten, die zur Berechnung der Lizenzcompliance in Ihrem Unternehmen verwendet werden.



Bei der Arbeit mit der SLM-Konsole werden Sie die meiste Zeit mit der Produktansicht **Überwacht** verbringen. Diese Ansicht zeigt die Produkte, die Sie aktiv überwachen wollen. Sobald Sie wichtige Produkte in diese Ansicht verschoben haben, kontrollieren Sie die Ansicht **Erkannt** auf eventuell vorhandene neue Produkte, die Ihre Aufmerksamkeit erfordern. Die Produkte, die Sie nicht überwachen müssen, können in die Ansicht **Ignoriert** verschoben werden, damit sie aus dem Weg sind.

Wenn Sie nicht sicher sind, wo sich ein Produkt befindet, öffnen Sie die Ansicht **Alle installierten Produkte** und suchen danach. Anschließend können Sie das Produkt in die entsprechende Ansicht (**Überwacht** oder **Ignoriert)** verschieben.

Öffnen der Konsole

Benutzer, deren Rollendefinition die Softwarelizenzüberwachung umfasst, können Daten in der Softwarelizenzüberwachungs-Konsole anzeigen und bearbeiten. Benutzern mit Administratorrechten wird diese Rolle standardmäßig zugewiesen. Anderen Benutzern können Berechtigungen zur Anzeige und zum Bearbeiten für die Rolle "Softwarelizenzüberwachung" erteilt werden.

Informationen darüber, wie Berechtigungen von Benutzer geändert werden, finden Sie unter "Verwalten von Rollen" auf Seite 46.

WICHTIG: Bei dem zum Anzeigen der SLM-Konsole verwendeten Browser darf die Funktion zum Blockieren von Popups nicht eingeschaltet sein. Ist diese Funktion eingeschaltet, sehen Sie unter Umständen Dialogfelder nicht, die von der SLM-Konsole geöffnet werden. Sollten Probleme bei der Anzeige von Elementen in der SLM-Konsole auftreten, vergewissern Sie sich, dass die Funktion für das Blockieren von Popups bei Ihrem Browser ausgeschaltet ist.

Funktionen

Die Softwarelizenzüberwachung umfasst folgende Funktionen:

- Leicht zugängliche Berichte zur Anwendungsnutzung und Lizenzcompliance.
- Freigabe von Produktlizenzen. Bei manchen Produkten kann eine neuere Version eine Lizenz an ältere Versionen leihen, so dass Ihre Geräte jederzeit lizenzkonform bleiben.
- Einfache Konfiguration der Lizenzparameter, einschließlich Informationen zum Erwerb, zum Lizenztyp, zur Menge und zur Seriennummer.
- Umfassende Berichterstellung, einschließlich Informationen darüber, wie oft jede lizenzierte Anwendung aufgerufen wurde, Datum der letzten Verwendung und Gesamtdauer der Anwendungsnutzung.
- Verfolgung der Installationen und Abgleich, einschließlich der von Ihnen verfolgte Elemente, wie Lizenzinhaber und physikalischer Standort des Geräts, auf dem die Lizenz installiert ist, sowie zusätzliche Notizen.
- Unterstützung mobiler Geräte. Der Agent überwacht die Nutzung mobiler Geräte, die vom Netzwerk getrennt werden und sendet diese Daten dann an den Coreserver, wenn das Gerät mit dem Netzwerk verbunden wird.
- Passive, minimale Bandbreite erfordernde Überwachung. Der Agent für die Softwarelizenzüberwachung überwacht passiv die Produktverwendung auf Geräten und belegt hierbei minimale Netzwerkbandbreite.
- Die automatische Produkterkennung scannt verwaltete Geräte auf installierte Anwendungen und zeichnet Daten auf der Basis der Dateien auf, die diesen Anwendungen zugeordnet sind.

Softwarelizenzüberwachungs-Tasks

Im Rahmen der Überwachung der Produktinstallation und Lizenznutzung führen Sie die folgenden allgemeinen Tasks aus.

Erfassen zuverlässiger Softwaredaten

Der Management Suite Softwareüberwachungsagent erfasst Inventardaten von verwalteten Geräten, die Aufschluss darüber geben, welche Softwareanwendungen installiert sind und wie oft diese ausgeführt werden. Diese Daten werden jedes Mal an den Coreserver übermittelt, wenn ein Softwareinventarscan abgeschlossen wurde. Bei der Überprüfung dieser Daten werden Sie möglicherweise feststellen, dass manche Anwendungen gar nicht gefunden oder nicht richtig erkannt wurden. Sie können die Softwarelizenzüberwachungs-Konsole dazu verwenden, Geräte auf bestimmte Software hin zu prüfen und, falls erforderlich, Produktinformationen hinzufügen oder korrigieren.

Auswählen der zu überwachenden Software

Wenn die Inventardaten in der Inventardatenbank gespeichert wurden, werden sie in der SLM-Konsole in der Produktansicht **Erkannt** angezeigt. Sie können dann die Produkte, die Sie überwachen möchten, aus dieser Liste auswählen und in die Ansicht **Überwacht** verschieben. Diese Produkte können mit Ihren Lizenzdaten verknüpft und in Berichten verfolgt werden, die Aufschluss darüber geben, inwieweit die Anzahl Ihrer Lizenzen mit der tatsächlichen Produktverwendung überstimmt. Die Produkte, die Sie nicht überwachen müssen, können in die Ansicht **Ignoriert** verschoben werden, damit sie aus dem Weg sind.

Hinzufügen von Lizenzdaten

Sie müssen Daten zu den Softwarelizenzen hinzufügen, die Sie überwachen möchten. Sie können diese Daten manuell hinzufügen oder Daten aus einer anderen Quelle importieren. Sobald Sie Informationen zu Ihren Lizenzen hinzugefügt haben, wie z. B. die Anzahl der erworbenen Arbeitsplatzlizenzen, Kaufdatum und Ablaufdatum, Lizenztypen und wie Lizenzen "verbraucht" werden, können Sie Compliancestatistiken und Berichte anzeigen, in denen die Lizenzdaten und die tatsächliche Softwarenutzung miteinander verglichen werden.

Erstellen von Berichten

Während Sie die Software- und Lizenzcompliancedaten prüfen, können Sie einen Bericht der jeweils angezeigten Daten generieren. Berichte können als CSV-Dateien, HTML-, PDF-, XML-, DOC-, XLS- oder Bilddateien formatiert werden.

Wenn Sie Lizenz- und Softwaredaten in der Datenbank eingerichtet haben, können Sie auch das Extra "Management Suite Berichte" verwenden, um vordefinierte Berichte mit Lizenz- und Nutzungsdaten zu generieren.

Voraussetzungen für den Einsatz der Softwarelizenzüberwachung

Bevor Sie die Softwarelizenzüberwachung verwenden können, sollten Sie die folgenden Tasks durchgeführt haben.

Der Inventardienst ist konfiguriert und wird ausgeführt

Die Softwarelizenzüberwachung setzt voraus, dass der LANDesk Agent auf den Geräten ausgeführt wird, die Sie überwachen möchten. Nach der Sammlung der Inventardaten werden in der SLM-Konsole in der Produktansicht **Erkannt** Produktdaten angezeigt. In dem Umfang, in dem Inventardaten hinzugefügt werden, wird die Ansicht **Erkannt** durch neue Produktdaten ergänzt. Dies findet zeitgleich mit den von Ihnen geplanten Inventarscans statt, die standardmäßig einmal pro Tag ausgeführt werden.

Gerätegruppen und Abfragen sind definiert

Wenn Sie Software auf Gruppen von Computern (statischen Gruppen) oder mittels Abfragen (dynamischen Gruppen) überwachen möchten, erstellen Sie diese in der Management Suite Netzwerkansicht. Die von Ihnen erstellten Gruppen und Abfragen sind dann in der Softwarelizenzüberwachungs-Konsole verfügbar. Dies macht es für Sie einfacher, installierte Produkte in Gruppen zu überprüfen, die Sie nach Standort, Unternehmensgruppe, Hardwaretyp oder einem beliebigen anderen Kriterium organisiert haben.

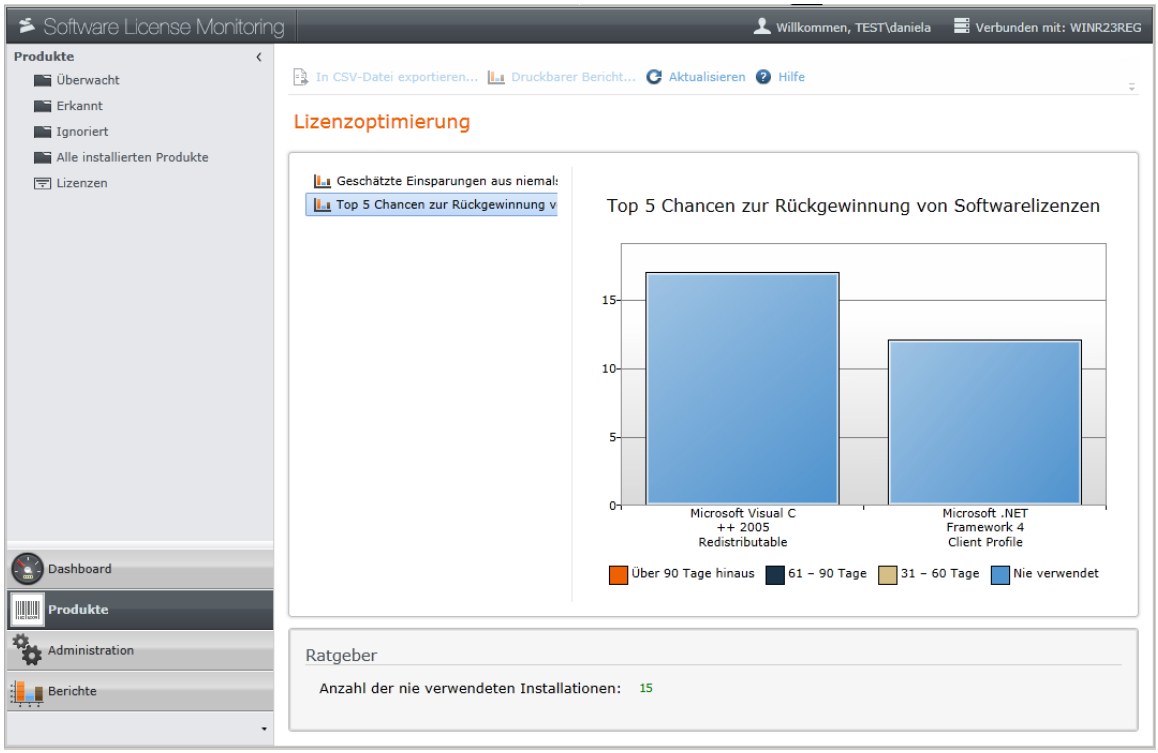
Softwarelizenzdaten sind verfügbar

Damit Sie die Konformität Ihres Unternehmens mit den Softwarelizenzbedingungen genau überwachen können, müssen Sie auf akkurate Lizenzdaten zugreifen können. Sie können Daten für mehrere Lizenzen importieren oder bei Bedarf einzelne Lizenzen hinzufügen. Wenn Sie sicher sind, dass die Lizenzdaten akkurat sind, können Sie unter Verwendung des Extras für die Softwarelizenzüberwachung mit der Überprüfung der Compliance beginnen.

Audit- und Compliancedaten im Dashboard

Das Dashboard zeigt aktuelle Übersichten zu wichtigen Audit- und Lizenzcompliancedaten. Die Dashboard-Seiten sind so konzipiert, dass Sie innerhalb kürzester Zeit auf nützliche Daten zugreifen können, die auf der Basis Ihrer Produkt-und Lizenzinformationen berechnet werden.

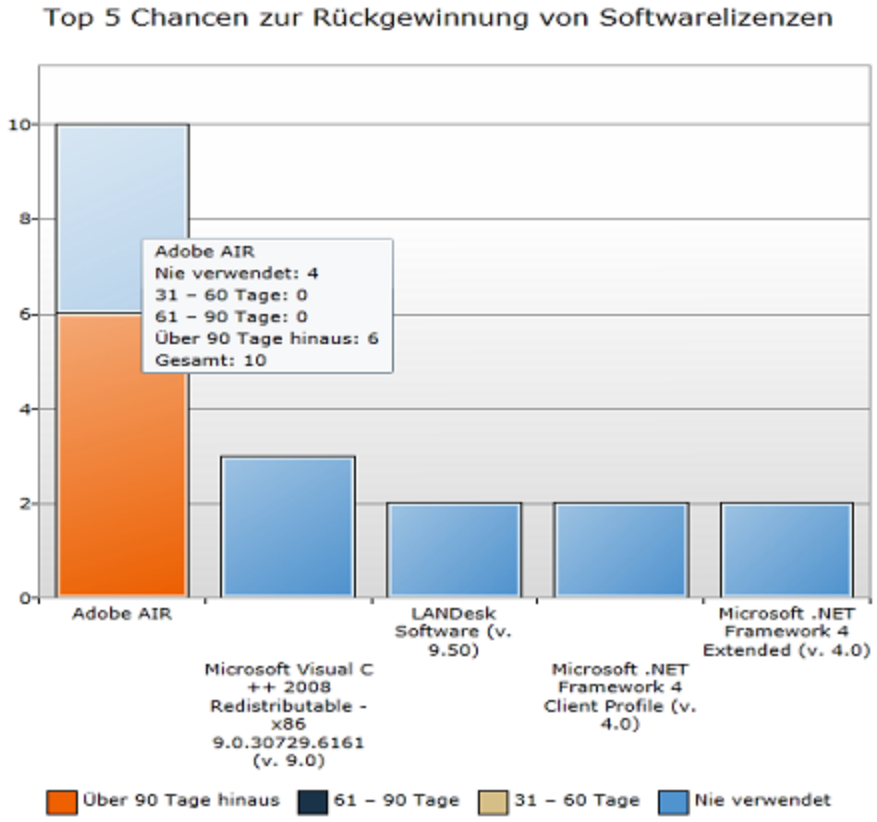
Dashboard-Seiten zeigen Berichtsübersichten mit Diagrammen und Daten des Ratgebers. Im folgenden Beispiel zeigt das Diagramm die fünf besten Chancen zur Rückgewinnung von Softwarelizenzen, die nicht genutzt werden. Das Ratgeberfeld unten in der Konsole zeigt die Gesamtzahl der installierten Produkte, die nie verwendet wurden.



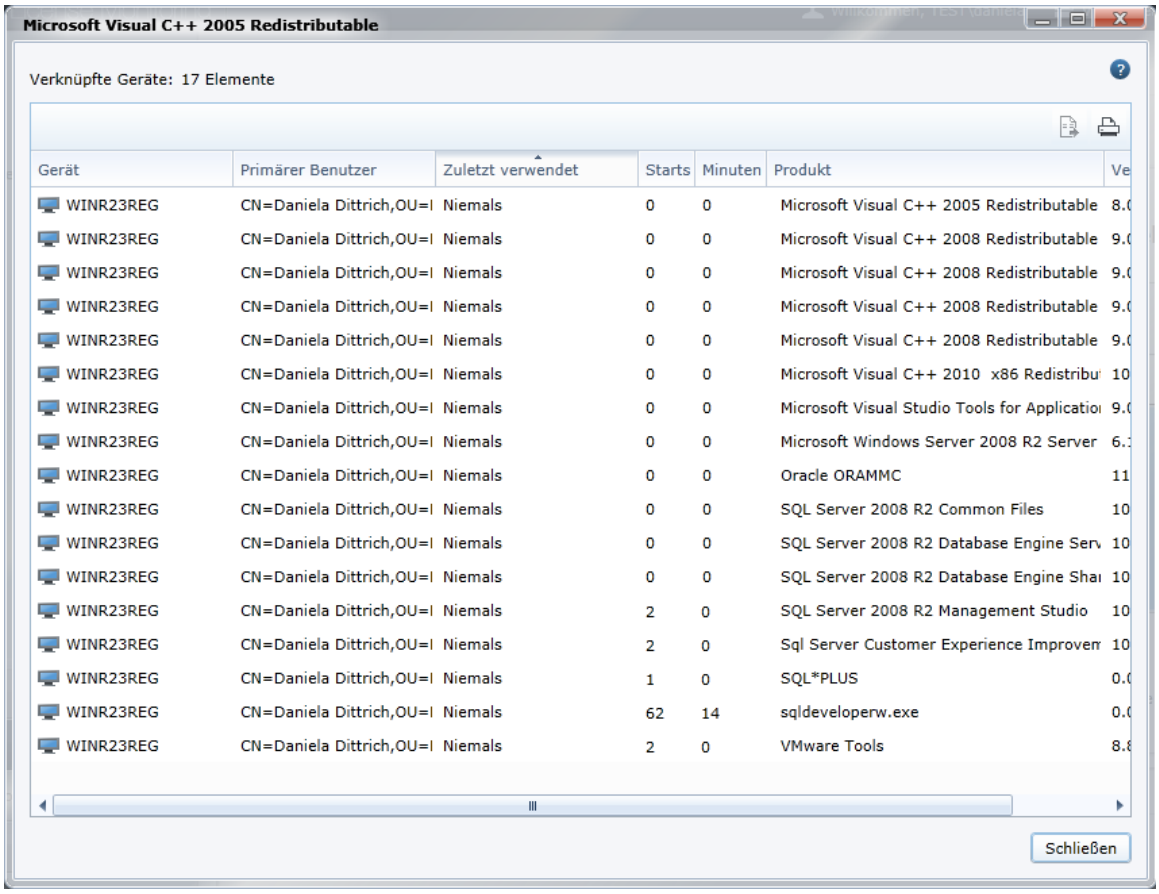
Der Abschnitt "Ratgeber" gibt Ihnen einen schnellen Überblick über Daten. Diagramme bieten zusätzliche Details und Sie können auf die einzelnen Abschnitte klicken, um Einzelheiten zu bestimmten Produkten anzuzeigen.

Anzeigen von Details zu Diagrammdaten

Wenn Sie auf einen Abschnitt des Diagramms zeigen, werden in einer Box die Daten zu diesem Abschnitt angezeigt

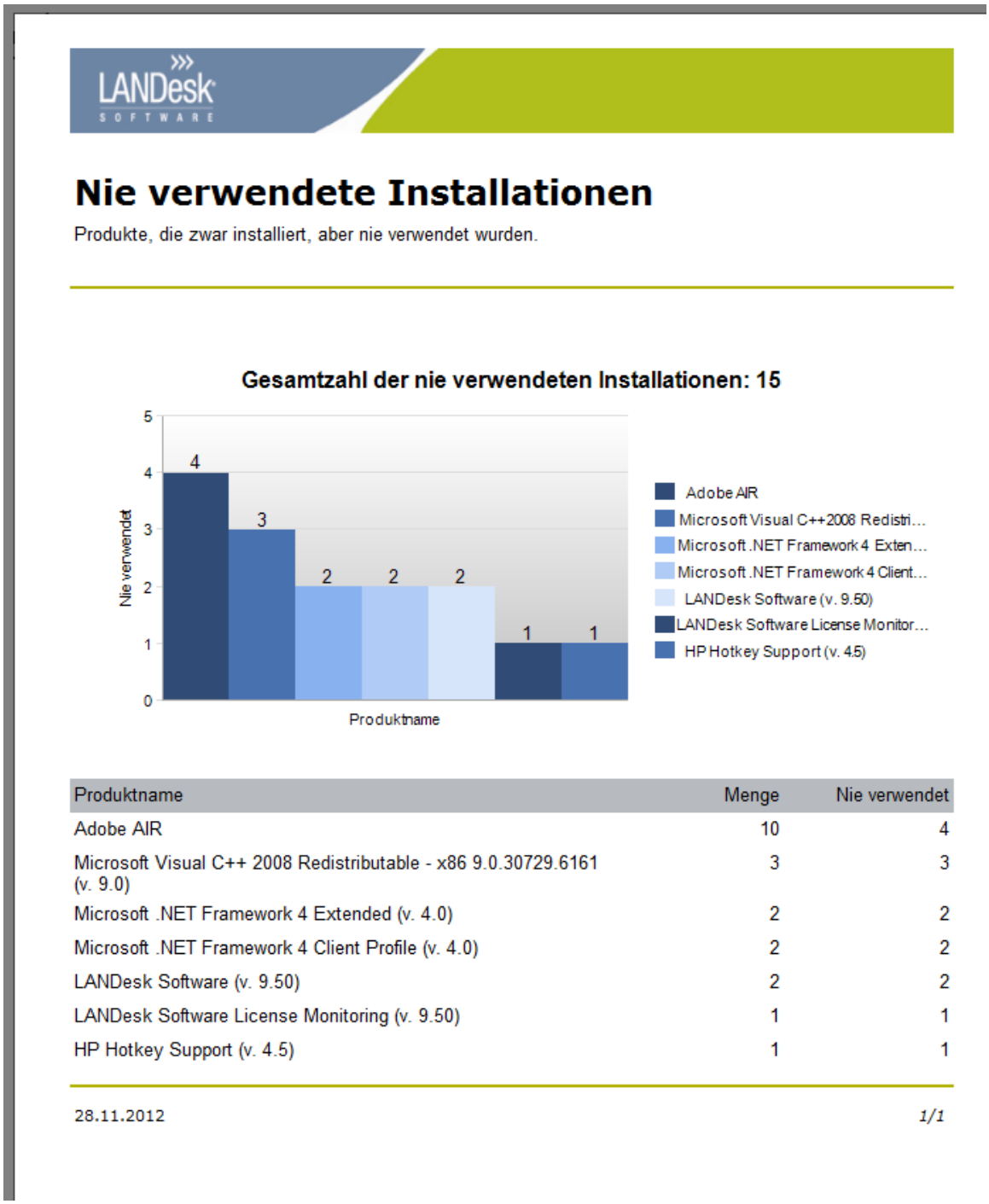


Klicken Sie auf einen Diagrammabschnitt, um eine Liste der zugehörigen Daten anzuzeigen. Wenn Sie beispielsweise im Diagramm zu den Chancen zur Softwarerückgewinnung auf einen Produktbalken klicken, wird eine Liste mit Computern angezeigt, auf denen dieses Produkt installiert ist.


Microsoft Visual C++ 2005 Redistributable
Verknüpfte Geräte: 17 Elemente
Gerät
Primärer Benutzer
Zuletzt verwendet
Starts
Minuten
Produkt
Ve
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2005 Redistributable 8.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2008 Redistributable 9.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2008 Redistributable 9.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2008 Redistributable 9.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2008 Redistributable 9.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual C++ 2010 x86 Redistribu 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Visual Studio Tools for Applicatio 9.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Microsoft Windows Server 2008 R2 Server 6.1
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 Oracle ORAMMC 11
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 SQL Server 2008 R2 Common Files 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 SQL Server 2008 R2 Database Engine Serv 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 0 0 SQL Server 2008 R2 Database Engine Shar 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 2 0 SQL Server 2008 R2 Management Studio 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 2 0 Sql Server Customer Experience Improver 10
WINR23REG CN=Daniela Dittrich,OU=I Niemals 1 0 SQL*PLUS 0.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 62 14 sqldeveloperw.exe 0.0
WINR23REG CN=Daniela Dittrich,OU=I Niemals 2 0 VMware Tools 8.8
Schließen

Anzeigen von Details zu Ratgeberdaten

Wenn die Ratgeberbox Daten enthält, klicken Sie auf die Zahl, um einen umfassenden Bericht der zugrunde liegenden Daten anzuzeigen. Im obigen Beispiel meldet der Ratgeber, dass 51 Installationen nie verwendet wurden. Klicken Sie auf den Zahlenwert 51, um einen Bericht anzuzeigen, der Aufschluss über die Produkte gibt, die in diese Gesamtzahl eingeflossen sind.



Nie verwendete Installationen

Produkte, die zwar installiert, aber nie verwendet wurden.

Gesamtzahl der nie verwendeten Installationen: 15

Produktname	Menge	Nie verwendet
Adobe AIR	10	4
Microsoft Visual C++ 2008 Redistributable - x86 9.0.30729.6161 (v. 9.0)	3	3
Microsoft .NET Framework 4 Extended (v. 4.0)	2	2
Microsoft .NET Framework 4 Client Profile (v. 4.0)	2	2
LANDesk Software (v. 9.50)	2	2
LANDesk Software License Monitoring (v. 9.50)	1	1
HP Hotkey Support (v. 4.5)	1	1

28.11.2012 *1/1*

Exportieren von Daten ins CSV-Format und in Berichte

Wenn Sie auf ein Diagramm klicken, um die Detaildaten anzuzeigen, oder wenn gerade ein Bildschirm mit Produktdetails angezeigt wird, können Sie Daten in eine CSV-Datei exportieren oder einen Bericht erstellen.

So exportieren Sie Daten ins CSV-Format

1. Klicken Sie auf einen Abschnitt des Diagramms.
2. Wählen Sie in dem neuen Fenster die Geräte aus, die Sie in die exportierten Daten einschließen möchten. (Klicken Sie innerhalb der Liste und drücken Sie **Strg+A**, um alle Geräte auszuwählen.
3. Klicken Sie auf die Schaltfläche **Exportieren**.
4. Geben Sie den Speicherort für die CSV-Datei an und klicken Sie anschließend auf **Speichern**.

So erstellen Sie einen Bericht zu ausgewählten Daten

1. Klicken Sie auf einen Abschnitt des Diagramms.
2. Wählen Sie in dem neuen Fenster die Geräte aus, die Sie in den Bericht einschließen möchten. (Klicken Sie innerhalb der Liste und drücken Sie **Strg+A**, um alle Geräte auszuwählen.
3. Klicken Sie auf die Schaltfläche **Bericht**.
4. Wählen in der Symbolleiste des Bericht-Viewers ein Format zum Speichern des Berichts aus und klicken Sie auf die Schaltfläche **Exportieren** .
5. Geben Sie den Speicherort für den Bericht an und klicken Sie anschließend auf **Speichern**.

Anzeigen des Dashboards "Audits"

Die Seite "Audits" des Dashboards bietet Berichte, die sich bei der Vorbereitung auf ein Audit Ihrer Softwarelizenznutzung als nützlich erweisen.

Bericht: Top-Installationen insgesamt

Dieser Bericht listet die fünf Produkte auf, die in Ihrem Unternehmen am häufigsten installiert sind. Hierbei wird die Anzahl der tatsächlichen Installationen und nicht die Anzahl der Geräte herangezogen, denn es könnte ja mehr als eine Installation auf einem Gerät vorliegen.

Ratgeber: Produkte und Lizenzen mit Auditkennzeichen

Dieser Bericht macht Sie auf Probleme aufmerksam, die während eines Softwarelizenzaudits gekennzeichnet werden könnten. Hierzu gehören Probleme mit der Lizenzdokumentation und Produkte, die noch nicht disponiert (in eine der beiden Gruppen "Überwacht" oder "Ignoriert" verschoben) wurden. Der Ratgeber zählt Elemente wie die folgenden:

- Lizenzen ohne Auftragsnummer
- Produkte ohne Lizenzen
- Erkannte Produkte, die nicht disponiert wurden
- Lizenzen ohne Herstellerrechnung

Klicken Sie auf ein Element, um einen vollständigen Bericht zu diesem Element anzuzeigen.

HINWEIS: Vordefinierte Berichte zu einzelnen Elementen mit Auditkennzeichen finden Sie außerdem im Extra "SLM-Berichte".

Anzeigen des Dashboards "Compliance"

Die Seite "Compliance" des Dashboards bietet Berichte, die Aufschluss über Produkte gibt, bei denen die Lizenzcompliance verletzt ist und die Ihre Aufmerksamkeit erfordern. Hierzu gehört eine Schätzung der Kosten, die entstehen, wenn Sie dafür sorgen, dass für alle Produkte eine gültige Lizenz vorliegt und damit Lizenzcompliance gegeben ist.

Bericht: Spitzenreiter "Lizenzcompliance verletzt" nach Installation

Dieses Diagramm zeigt bis zu fünf Produkte mit der größten Anzahl von nicht lizenzierten Installationen.

Bericht: Spitzenreiter "Lizenzcompliance verletzt" nach Kosten der Lizenzanpassung ("True-Up")

Dieses Diagramm zeigt die Produkte, bei denen die höchsten Kosten anfallen, um Compliance zu erreichen. Die Berechnungsgrundlage hierfür ist die Anzahl der nicht lizenzierten Installationen multipliziert mit den mit diesem Produkt verknüpften Stückkosten.

Bericht: Spitzenreiter "Lizenzcompliance verletzt" nach Hersteller

In diesem Diagramm werden Produkte nach Herstellern gruppiert. Es gibt Aufschluss darüber, für welche Herstellerprodukte am meisten nicht lizenzierten Installationen vorliegt. Dies ist bei der Identifizierung von Compliance-Anforderungen hilfreich, wenn ein Audit mit einem Hersteller ansteht und Sie verifizieren müssen, dass die Installation den Bestimmungen Ihrer Lizenz für diesen Hersteller entspricht.

Ratgeber: Geschätzte Compliance-Kosten

Die geschätzten Gesamtkosten, die entstehen, wenn Sie dafür sorgen, dass die Lizenzanforderungen bei allen Produkten erfüllt sind. Die Berechnungsgrundlage hierfür ist die Anzahl der nicht lizenzierten Produkte multipliziert mit den mit dem jeweiligen Produkt verknüpften Stückkosten.

Ratgeber: Produkte, bei denen die Lizenzcompliance verletzt ist

Die Anzahl der Produkte, bei denen die Compliance-Anforderungen der verknüpften Lizenz nicht erfüllt sind. Klicken Sie auf die Zahl, um eine vollständige Liste der Produkte mit Compliance-Verletzung anzuzeigen.

Anzeigen des Dashboards "Lizenzoptimierung"

Die Seite "Lizenzoptimierung" bietet Berichte mit Schätzwerten für Einsparungen, die durch das Entfernen nicht verwendeter Lizenzen von Computern in Ihrem Unternehmen erzielt werden können. Bei diesen Berichten steht installierte Software im Mittelpunkt, die nie verwendet wurde oder für ein bestimmte Zeit nicht verwendet wurde.

HINWEIS: Produkte gelten als "nie verwendet", wenn in den Inventardaten für die Dauer, für die das Produkt ausgeführt wurde, der Wert "0" zurückgegeben wird. Es ist jedoch möglich, dass ein Produkt installiert ist und die Person, die es verwendet, die Anwendung einmal gestartet und nach weniger als einer Minute wieder geschlossen hat. In diesem Fall wird das Produkt im Dashboard und in den Berichte trotzdem als "nie verwendet" geführt.

Bericht: Geschätzte Einsparungen aus niemals genutzten Anwendungen

Dieser Bericht listet die fünf nie verwendeten Produkte auf, deren Entfernen für Ihr Unternehmen die größten Einsparungen bringen würde. Die Berechnungsgrundlage hierfür ist die Anzahl der nie verwendeten Produkte multipliziert mit den mit diesem Produkt verknüpften Stückkosten.

Bericht: Top 5 Chancen zur Rückgewinnung von Softwarelizenzen

Dieser Bericht listet die fünf Produkte mit der höchsten Anzahl von nie verwendeten oder selten verwendeten Installationen auf. Dabei erfolgt keine Kostenschätzung, sondern eine Auflistung von Computern mit dem jeweiligen Produkt, auf denen das Produkt innerhalb einer bestimmten Anzahl von Tagen nicht verwendet wurde (31 bis 60, 61 bis 90, mehr als 90 Tage oder nie verwendet).

Ratgeber: Anzahl der nie verwendeten Installationen

Dieser Bericht liefert die Gesamtzahl der Instanzen, bei denen installierte Software nie verwendet wurde. Der Bericht listet alle Produkte mit der jeweiligen Gesamtzahl der Installationen auf und zeigt auf, in wie vielen Fällen das Produkt niemals verwendet wurde.

Überwachen der Softwarenutzung

Der Softwareüberwachungsscan von LANDesk Management Suite wird ausgeführt, wenn Sie regelmäßige Inventarscans planen. Er überwacht die aktiven ausführbaren Dateien und vergleicht die Anwendungsinformationen auf jedem Gerät mit den Namen und den Dateigrößen der in der Datenbank gespeicherten ausführbaren Dateien.

Zwei weitere Inventarscans liefern zusätzliche Daten über Software und vervollständigen damit das Gesamtbild. Diese Scans prüfen die Windows-Registrierung, Deinstallationsschlüssel, .msi-Dateien, Shortcuts und GUIDs, um Softwareprodukte zu identifizieren. All Scandaten werden dann verglichen, damit sich ein möglichst vollständiges Bild ergibt, welche Software auf welchem verwalteten Gerät installiert ist.

Die Softwarelizenzüberwachungs-Konsole (SLM-Konsole) zeigt diese Datenübersicht in der Ansicht "Produkte" an. Selbst wenn Ihnen keine Lizenzdaten zur Verfügung stehen, können Sie diese Produktdaten anzeigen, um herauszufinden, auf wie vielen verwalteten Geräten ein Softwareprodukt erkannt wurde.

Überwachen und Ignorieren von Produkten

Wenn Sie die SLM-Konsole das erste Mal öffnen, finden Sie alle erkannten Produkte in der Produktansicht **Erkannt**. Im Rahmen der Verwaltung der Software- und Lizenznutzung können Sie festlegen, für welche Software eine Überwachung wichtig ist. Software, die Sie verfolgen möchten, können Sie in die Produktansicht **Überwacht** verschieben. Andere Softwareanwendungen sind vielleicht nicht so wichtig für Sie und können daher in die Produktansicht **Ignoriert** verschoben werden. Sie werden damit nicht in die Berechnungen für Produkte einbezogen, die die Lizenzcompliance verletzen.

So überwachen Sie ein Softwareprodukt

1. Klicken Sie auf **Produkte > Erkannt**.
2. Verwenden Sie das Feld **Suchen**, um ein Produkt zu finden
3. Klicken Sie auf das Produkt. Klicken Sie in der Symbolleiste auf **Aktionen > Verschieben nach > Überwacht**.

Das Produkt ist jetzt in der Produktansicht **Überwacht** aufgeführt.

HINWEIS: Sie können auch mit der rechten Maustaste auf ein Produkt klicken und dann auf **Verschieben nach > Überwacht** klicken.

So ignorieren Sie ein Softwareprodukt oder eine Softwareproduktgruppe

1. Klicken Sie auf **Produkte > Erkannt**.
2. Verwenden Sie das Feld **Suchen**, um ein Produkt zu finden
3. Klicken Sie auf das Produkt. Klicken Sie in der Symbolleiste auf **Aktionen > Verschieben nach > Ignoriert**.

Das Produkt ist jetzt in der Produktansicht **Ignoriert** aufgeführt.

HINWEIS: Sie können auch mit der rechten Maustaste auf ein Produkt klicken und dann auf **Verschieben nach > Ignoriert** klicken.

Suchen eines Produkts

Das in den Produktansichten enthaltene Suchfeld ermöglicht ein schnelles Auffinden von Produkten. Für einen Suchlauf müssen Sie mindestens zwei Zeichen eingeben. Die Suchergebnisse, die der von Ihnen eingegebenen Zeichenfolge entsprechen, werden in den Spalten "Produkt" oder "Hersteller" anzeigt.

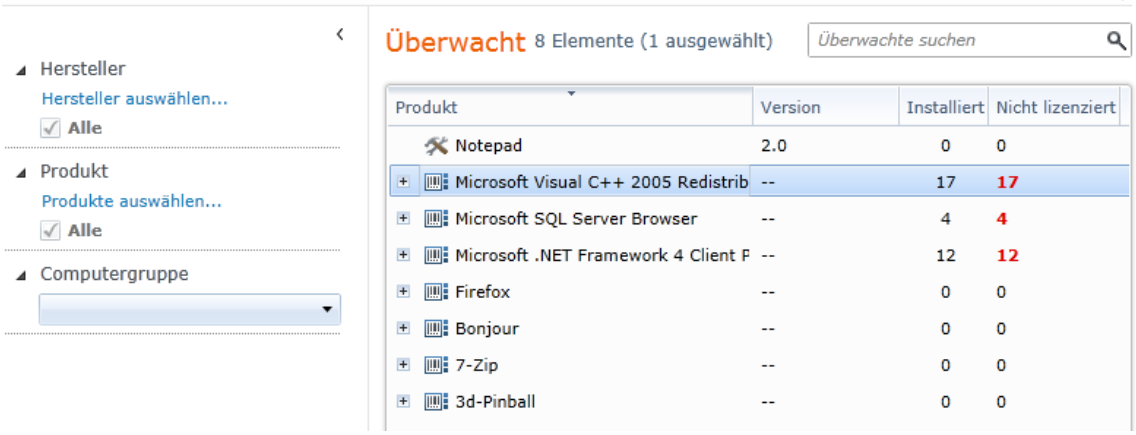
So verwenden Sie das Feld "Suche", um ein Produkt zu finden

1. Klicken Sie auf **Produkte** und öffnen Sie eine der Ansichten (Überwacht, Erkannt, Ignoriert oder Alle).
2. Geben Sie in das Feld **Suche** mindestens zwei Zeichen ein und drücken Sie die **Eingabetaste**.

   Die Liste enthält alle Produkte bzw. Hersteller, die der von Ihnen eingegebenen Zeichenfolge entsprechen.
3. Wählen Sie ein oder mehrere Listenelemente aus und klicken Sie entweder auf eine Schaltfläche der Symbolleiste oder mit der rechten Maustaste auf die Elemente, um auf sie einzuwirken. Sie können die Elemente in eine andere Ansicht ziehen, um sie zu verschieben.
4. Um alle Produkte in der Liste wieder anzuzeigen, klicken Sie auf das **X** im Suchfeld, um die Suche zu löschen.

Erweiterte Produktsuche

Die Liste einer Produktansicht können Sie filtern, indem Sie einen Hersteller, ein Produkt oder eine Computergruppe als Filter auswählen. Sie können einen oder mehrere dieser Filter zum Anzeigen einer geringeren Anzahl von Produkten in einer Liste verwenden. Diese Filter finden Sie in der Spalte links neben der Produktliste.

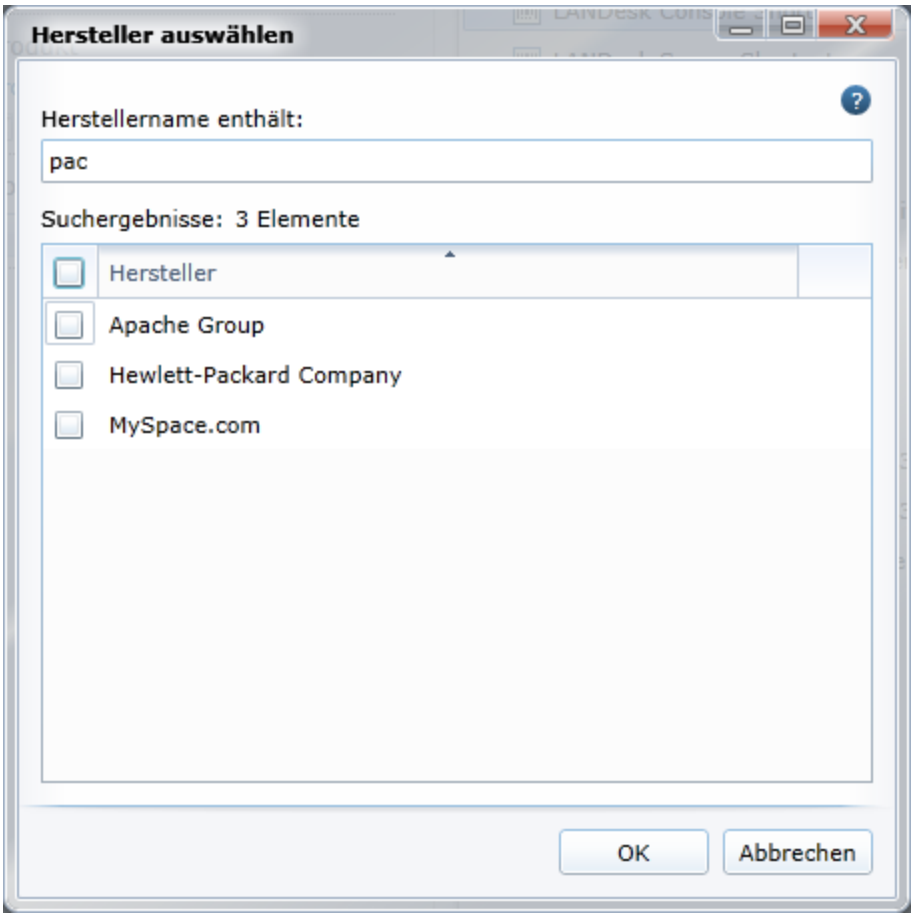


- Wählen Sie einen **Hersteller** (oder einen normalisierten Hersteller) aus, um nur jene Produkte anzuzeigen, die mit diesem Hersteller verknüpft sind.
- Wählen Sie ein **Produkt** (oder ein normalisiertes Produkt) aus, um nur jene Produkte anzuzeigen, die mit diesem Produktnamen übereinstimmen.
- Wählen Sie eine **Computergruppe** aus, um nur diejenigen Produkte anzuzeigen, die auf Computern in dieser Gruppe installiert sind. Dies ist nützlich, wenn Sie Produkte finden wollen, von denen Sie wissen, dass sie auf einer bestimmten Gruppe von Computern in Ihrem Unternehmen installiert sind.

So filtern Sie eine Produktsuche nach Hersteller

1. Klicken Sie auf **Produkte** und öffnen Sie eine der Ansichten (Überwacht, Erkannt, Ignoriert oder Alle).
2. Klicken Sie der Spalte links neben der Liste auf **Hersteller auswählen**.

3. Geben Sie mindestens drei Zeichen in das Feld **Herstellername** ein. Übereinstimmende Namen werden im Feld **Suchergebnisse** aufgeführt.

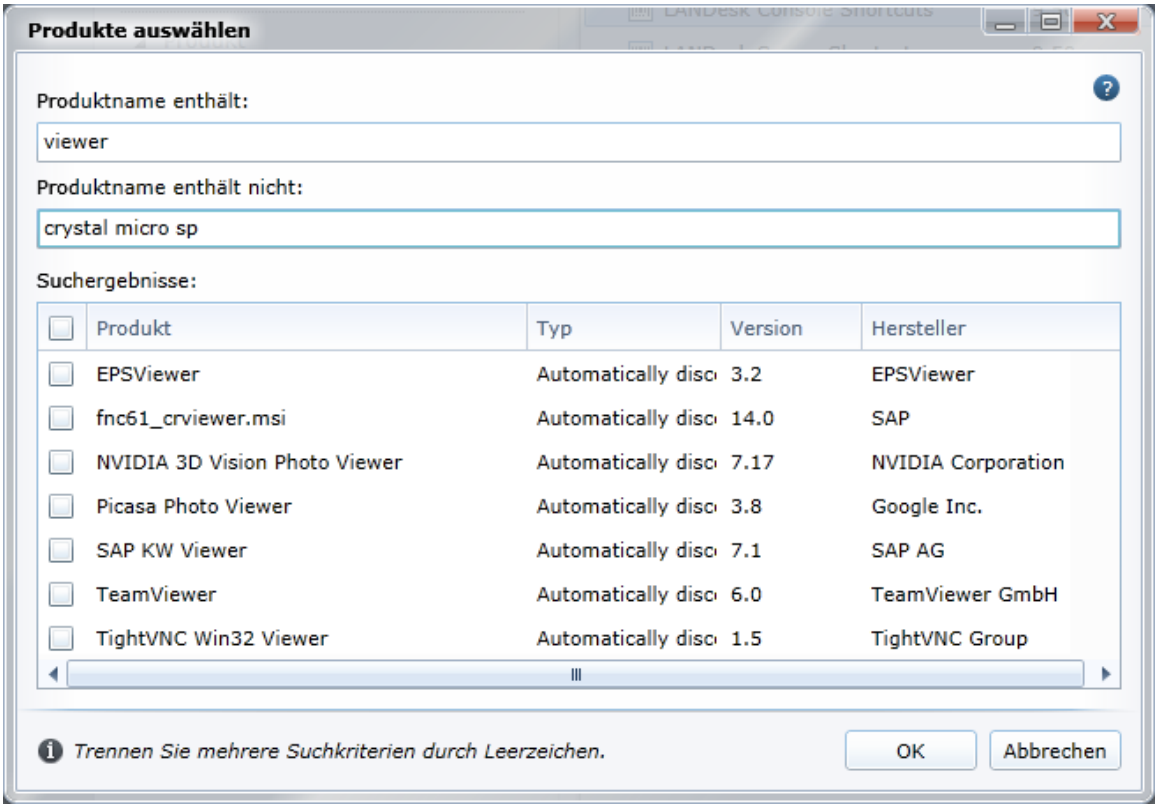


4. Wählen Sie die Herstellernamen aus, die Sie als Filter verwenden möchten, und klicken Sie auf **OK**.

So filtern Sie eine Produktsuche nach Produktname

1. Klicken Sie auf **Produkte** und öffnen Sie eine der Ansichten (Überwacht, Erkannt, Ignoriert oder Alle).
2. Klicken Sie der Spalte links neben der Liste auf **Produkte auswählen**.

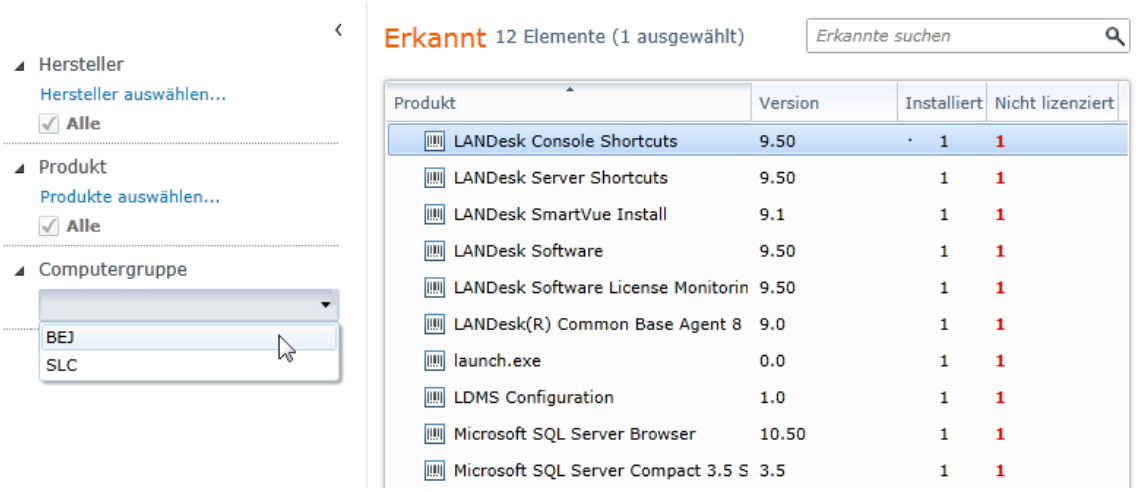
3. Geben Sie mindestens drei Zeichen in das Feld **Produktname** ein. Übereinstimmende Namen werden im Feld **Suchergebnisse** aufgeführt. Sie können auch Zeichenfolgen angeben, die aus den Suchergebnisse ausgeschlossen werden sollen. Hierzu geben Sie eine oder mehrere, durch Leerzeichen getrennte Zeichenfolgen in das Feld **Produktname enthält nicht** ein. Damit können Sie unter Umständen die Anzahl der Suchergebnisse reduzieren.



4. Wählen Sie die Produktnamen aus, die Sie als Filter verwenden möchten, und klicken Sie auf **OK**.

So filtern Sie eine Produktsuche nach einer Computergruppe

1. Klicken Sie auf **Produkte** und öffnen Sie eine der Ansichten (Überwacht, Erkannt, Ignoriert oder Alle).
2. Klicken Sie in der Spalte links neben der Liste auf die Liste **Computergruppe** und wählen Sie eine Computergruppe aus.



Die Liste ändert sich dahingehend, dass nur Produkte angezeigt werden, die auf den Computern in der von Ihnen ausgewählten Gruppe installiert sind.

3. Um den Filter zu entfernen und alle Produkte anzuzeigen, klicken Sie auf **Zurücksetzen**.

Anzeigen aller installierten Produkte

Nachdem Sie die Produkte den Kategorien "Überwacht" und "Ignoriert" zugeordnet haben, müssen Sie eventuell eines dieser Produkte wiederfinden, erinnern sich jedoch nicht mehr daran, welcher Gruppe Sie es zugeordnet haben. Sie können die Ansicht **Alle installierten Produkte** verwenden und alle erkannten Produkte durchsuchen.

So zeigen Sie alle installierten Produkte an

1. Klicken Sie auf **Produkte**.
2. Klicken Sie auf **Alle installierten Produkte**.
3. Verwenden Sie das Feld **Suchen** oder Filter, um das gewünschte Produkt zu finden.
4. In welcher Produktansicht das Produkt enthalten ist, können Sie anhand der Spalte **Status** ablesen. Sie zeigt an, ob es sich bei dem Produkt um ein überwachtes, erkanntes oder ignoriertes Produkt handelt.

Erstellen von benutzerdefinierten Produkten

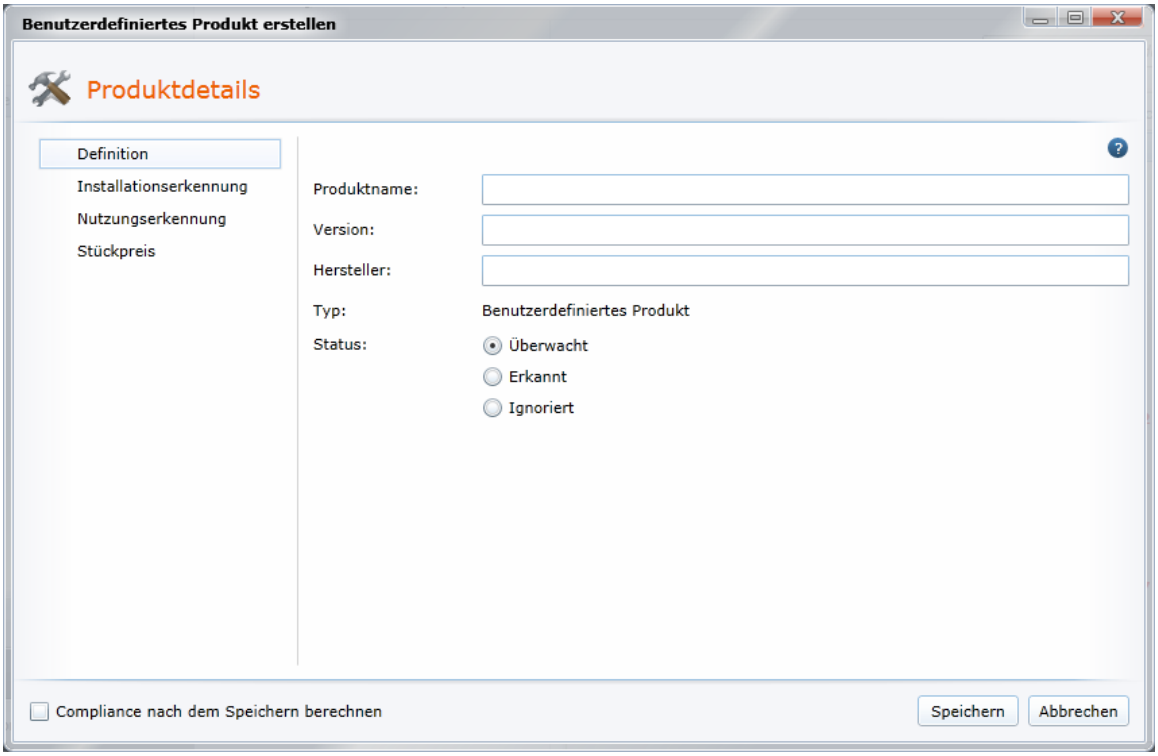
Sie können benutzerdefinierte Produkte für nicht identifizierte oder nicht korrekt identifizierte ausführbare Softwaredateien erstellen. Dabei werden die im benutzerdefinierten Produkt enthaltenen Dateien automatisch zur Liste der Dateien hinzugefügt, nach denen der Inventarscanner sucht.

Sie können angeben, welche Dateien darauf hinweisen, dass Software installiert wurde, und Sie können auch Verwendungsdateien definieren, die anzeigen, dass die Software auf einem Computer verwendet wird.

In manchen Fällen ist es angebracht, eine Management Suite Abfrage zu verwenden, um die installierten Produkte zu finden. Beispielweise wenn ein Produkt anhand der ausführbaren Dateien nicht korrekt identifiziert werden kann, dafür aber anhand von Inventardaten, die Sie zu einer Abfrage hinzufügen können.

So erstellen Sie eine benutzerdefinierte Produktdefinition

1. Klicken Sie auf **Produkte** und anschließend auf eine der Produktansichten.
2. Klicken Sie in der Symbolleiste auf **Neu > Benutzerdefiniertes Produkt**.



3. Geben Sie einen Namen in das Feld **Produktname** ein.
4. Geben Sie in das Feld **Version** eine Nummer oder eine Nummer und ein Platzhalterzeichen ein.
5. Geben Sie mindestens drei Zeichen in das Feld **Hersteller** ein, um Namen mit den entsprechenden Zeichen anzuzeigen. Wählen Sie den Herstellernamen aus.
6. Wählen Sie unter **Status** entweder **Überwacht** oder **Ignoriert** aus, um dieses neue Produkt in einer dieser Produktansichten aufzulisten. (Ein benutzerdefiniertes Produkt wird standardmäßig in die Ansicht der überwachten Produkte verschoben.)
7. Klicken Sie auf **Installationserkennung**.

8. Wenn Sie die Produkterkennung auf der Basis einer Management Suite Abfrage ausführen wollen, wählen Sie **Abfrageerkennung verwenden**. Klicken Sie auf **Durchsuchen** und wählen Sie eine Abfrage aus, die Sie in der Management Suite Netzwerkansicht erstellt haben. Alle Geräte, die dieser Abfrage entsprechen, werden als Geräte zurückgegeben, die mit diesem Produkt übereinstimmen.
9. Wählen Sie **Dateierkennung verwenden** aus, um Produkte anhand der installierten Dateien zu erkennen. Die Dateinamen, die Sie hier hinzufügen, bestimmen, wie das Produkt bei Inventarscans erkannt wird.
10. Klicken Sie auf die Schaltfläche **Hinzufügen (+)**. Im Dialogfeld **Dateien hinzufügen** können Sie entweder einen (in der Inventardatenbank) vorhandenen Dateinamen auswählen oder auf **Neue Datei definieren** klicken und den Dateinamen, die Größe der Datei und die Versionsnummer der Produktdatei eingeben. Wiederholen Sie den Vorgang für alle Produktdateien, die Sie verwenden möchten. Klicken Sie abschließend auf **OK**.
11. Wählen Sie **Alle abgleichen** oder **Beliebige abgleichen**, um anzugeben, ob alle Dateien gefunden werden müssen oder ob es reicht, wenn mindestens eine Datei gefunden wird.
12. Klicken Sie auf **Nutzungserkennung**. Verwenden Sie diese Option, um die Dateien einzuschließen, die darauf hinweisen, dass das Produkt verwendet wird.
13. Klicken Sie auf die Schaltfläche **Hinzufügen (+)**. Im Dialogfeld **Datei hinzufügen** können Sie entweder einen (in der Inventardatenbank) vorhandenen Dateinamen auswählen oder auf **Neue Datei definieren** klicken und den Dateinamen, die Größe der Datei und die Versionsnummer der Produktdatei eingeben. Wiederholen Sie den Vorgang für alle Produktdateien, die Sie verwenden möchten. Klicken Sie abschließend auf **OK**.
14. Klicken Sie auf **Stückpreis**. Wählen Sie ein Verfahren zur Berechnung des Stückpreises aus.
    - Wählen Sie **Automatisch berechneten Stückpreis in allen Berechnungen verwenden**, wenn es mehrere Lizenzen mit unterschiedlichen Stückpreisen für dieses Produkt gibt. Wenn Sie diese Option auswählen, wird als Stückpreis der Durchschnitt aller Stückpreise der verschiedenen Lizenzen verwendet.
    - Wählen Sie **Geben Sie einen Stückpreis an**, wenn Sie denselben Stückpreis in sämtlichen Berechnungen verwenden wollen. Wenn Sie beispielsweise zwei Lizenzen mit unterschiedlichen Preisen für ein und dasselbe Produkt haben und den höheren der beiden Preise in Berechnungen verwenden möchten, können Sie diesen Stückpreis hier angeben.
15. Wenn Sie Produktinformationen hinzufügen, die einen Einfluss auf die Lizenz- und Nutzungsberechnung haben, beispielsweise wenn ein Produkt mit einer Lizenz verknüpft ist, das Sie aktiv überwachen, aktivieren Sie das Kontrollkästchen **Compliance nach dem Speichern berechnen**, um eine Neuberechnung zu initiieren, damit die Complianceberichte aktuelle Informationen enthalten.
16. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

WICHTIG: Die beiden Arten von Erkennungsdateien, d .h. zur Installation und zur Verwendung, werden beide zur Sammlung von Produktdaten mit Inventarscans benötigt. Installationsdateien zeigen an, dass eine Datei installiert wurde und dienen daher zur Bestimmung, ob ein Softwareprodukt auf einem Computer vorhanden ist. Verwendungsdaten zeigen an, dass die Software ausgeführt wurde und dienen daher zur Bestimmung, ob ein installiertes Produkt benutzt wurde.

Wenn das Inventar eines Computers eine Übereinstimmung mit den Installationsdateien aufweist, meldet SLM, dass die Software installiert ist. Wenn jedoch keine Verwendungsdateien für das Produkt angegeben sind, wird SLM stets melden, dass das Produkt niemals benutzt wurde. Bei der Erstellung eines

benutzerdefinierten Produkts sollten Sie sicherstellen, dass Sie mindestens eine Verwendungsdatei definieren, damit SLM korrekt melden kann, ob das Produkt jemals verwendet wurde.

Bearbeiten eines erkannten Produkts

1. Klicken Sie auf **Produkte > Erkannt**.
2. Suchen Sie das Produkt mithilfe des Felds **Suchen** oder dem Filter **Produkte auswählen**.
3. Wählen Sie das Produkt aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Bearbeiten**.

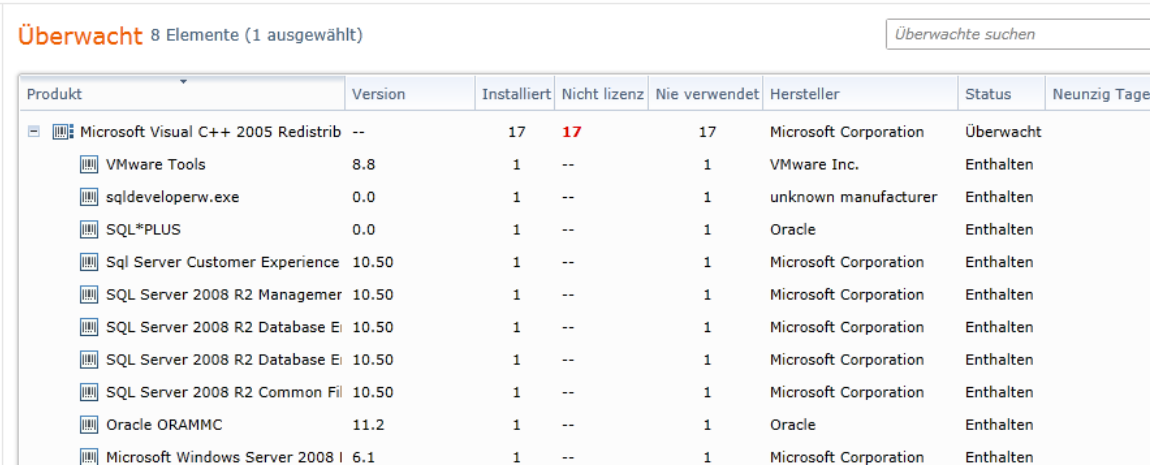
   Das Dialogfeld **Produktdetails bearbeiten** wird aufgerufen. Einige Elemente sind schreibgeschützt, andere können bearbeitet werden.
4. Wählen Sie unter **Status** entweder **Überwacht** oder **Ignoriert** aus, um dieses neue Produkt in einer der Produktansichten aufzulisten.
5. Klicken Sie auf **Installationserkennung**. Beachten Sie, dass alle Optionen schreibgeschützt sind.
6. Klicken Sie auf **Nutzungserkennung**. Sie können Dateien hinzufügen, die darauf hinweisen, dass das Produkt verwendet wird.
7. Klicken Sie auf die Schaltfläche **Hinzufügen (+)**. Im Dialogfeld **Dateien hinzufügen** können Sie entweder einen (in der Inventardatenbank) vorhandenen Dateinamen auswählen oder auf **Neue Datei definieren** klicken und den Dateinamen, die Größe der Datei und die Versionsnummer der Produktdatei eingeben. Wiederholen Sie diese Schritte für alle Produktdateien, die Sie verwenden möchten, um zu bestimmen, ob das Produkt verwendet wird. Klicken Sie abschließend auf **OK**.
8. Klicken Sie auf **Stückpreis**. Ist eine Bearbeitung der Optionen möglich, können Sie den Stückpreis ändern, der zur Berechnung des Kostenaufwands zum Erreichen von Lizenzcompliance verwendet wird.
9. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

Erstellen eines normalisierten Produkts

Bei der Überprüfung Ihrer Produktdaten werden Sie unter Umständen feststellen, dass ein und dasselbe Produkt durch mehrere Instanzen des Produkts und der Versionsnummer dargestellt wird. Sie können Produkte normalisieren, sodass ein Produktname und eine Versionsnummer anstelle der vielen Varianten von Produktname und Version verwendet wird.

Beispielsweise könnten auf den diversen Computern in Ihrem Unternehmen verschiedene Versionen von Adobe Reader installiert sein. Wenn eine getrennte Verfolgung älterer Versionsnummern für Sie nicht wichtig ist, können Sie alle Instanzen von Adobe Reader 7, 8 und 9 in der Produktansicht **Erkannt** auswählen und als "Adobe Reader" normalisieren Wenn Sie verfolgen möchten, auf wie vielen Computern Version X installiert ist, können Sie alle Instanzen von Adobe Reader X (zum Beispiel die Versionsnummer 10.0 und die Versionsnummer 10.1) auswählen und als "Adobe Reader X" normalisieren.

Ein normalisiertes Produkt wird mit einem Pluszeichen (+) vor dem Produktnamen angezeigt. Klicken Sie auf das Pluszeichen, um das Produkt zu erweitern und alle enthaltenen Varianten anzuzeigen.



Produkt	Version	Installiert	Nicht lizenz	Nie verwendet	Hersteller	Status	Neunzig Tage
Microsoft Visual C++ 2005 Redistrib	--	17	17	17	Microsoft Corporation	Überwacht	
VMware Tools	8.8	1	--	1	VMware Inc.	Enthalten	
sqldeveloperw.exe	0.0	1	--	1	unknown manufacturer	Enthalten	
SQL*PLUS	0.0	1	--	1	Oracle	Enthalten	
Sql Server Customer Experience	10.50	1	--	1	Microsoft Corporation	Enthalten	
SQL Server 2008 R2 Managemer	10.50	1	--	1	Microsoft Corporation	Enthalten	
SQL Server 2008 R2 Database E	10.50	1	--	1	Microsoft Corporation	Enthalten	
SQL Server 2008 R2 Database E	10.50	1	--	1	Microsoft Corporation	Enthalten	
SQL Server 2008 R2 Common Fil	10.50	1	--	1	Microsoft Corporation	Enthalten	
Oracle ORAMMC	11.2	1	--	1	Oracle	Enthalten	
Microsoft Windows Server 2008 I	6.1	1	--	1	Microsoft Corporation	Enthalten	

So erstellen Sie ein normalisiertes Produkt

1. Klicken Sie auf **Produkte** und klicken Sie dann auf eine der Produktansichten (Überwacht, Erkannt, Ignoriert oder Alle installierten Produkte).
2. Suchen Sie unter Verwendung des Felds **Suchen** die Produktnamen, die Sie kombinieren möchten.
3. Wählen Sie die Produktnamen aus und klicken Sie auf **Aktionen > Gruppe**.
4. Bearbeiten Sie den Namen, den Sie für das normalisierte Produkt verwenden möchten.
5. Wählen Sie den Status aus, unter dem das Produkt aufgeführt werden soll (**Überwacht** oder **Ignoriert**).
6. Klicken Sie auf **Speichern**.

Der von Ihnen gewählte Name erscheint in der von Ihnen ausgewählten Produktansicht. Ein Pluszeichen (+) neben dem Namen zeigt an, dass es sich um ein normalisiertes Produkt handelt. Wenn Sie den Namen erweitern (indem Sie auf + klicken), werden alle Namen angezeigt, die für diesen normalisierten Namen zusammengruppiert wurden.

So fügen Sie automatisch Produkte zu einem normalisierten Produkt hinzu.

1. Klicken Sie auf **Produkte** und klicken Sie dann auf eine der Produktansichten (Überwacht, Ignoriert oder Alle installierten Produkte).
2. Klicken Sie in der Symbolleiste auf **Neu > Normalisiertes Produkt**. (Wenn Sie Produkte zu einem vorhandenen normalisierten Produkt hinzufügen möchten, wählen Sie das Produkt aus und klicken Sie dann in der Symbolleiste auf **Bearbeiten**.
3. Geben Sie den Namen ein, den Sie für das normalisierte Produkt verwenden möchten.
4. Wählen Sie den Status aus, unter dem das Produkt aufgeführt werden soll (**Überwacht** oder **Ignoriert**).
5. Klicken Sie auf **Dynamische Regeln**.
6. Geben Sie eine Regel in das Feld ein. Verwenden Sie das Sternchen (*) als Platzhalter in der Suche nach Übereinstimmungen.
7. Um eine weitere Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** [+] und geben eine weitere Regel ein.
8. Klicken Sie auf **Speichern**, nachdem alle Regeln hinzugefügt wurden.

Derzeit in der Datenbank enthaltene Produktnamen, die mit den Regeln übereinstimmen, werden im Feld **Übereinstimmende Produkte** aufgelistet. Werden nun neue Inventardaten und andere Produktnamen zur Datenbank hinzugefügt, so werden diese Namen automatisch unter dem Namen des normalisierten Produkts eingeschlossen.

HINWEIS: Bei manchen normalisierten Produkten können Sie auf der Seite **Definition** einen einzigen Herstellernamen angeben. Manche normalisierte Namen umfassen jedoch Produkte mit verschiedenen Varianten des Herstellernamens. In diesem Fall verwenden Sie eine teilweise übereinstimmende Zeichenfolge mit einem Platzhalterzeichen, damit alle Varianten eingeschlossen sind. Wenn Sie beispielsweise alle Varianten von "Adobe Systems" als Hersteller einschließen wollen, geben Sie **Adobe*** in das Feld Hersteller ein.

Löschen eines normalisierten Produkts

Sie können ein normalisiertes Produkt löschen, indem Sie es auswählen und die Taste **Entf** drücken. Wenn Sie dies tun, werden die einzelnen Produkte, die zusammengruppiert wurden als Einzelprodukte zurück in die Produktliste überführt.

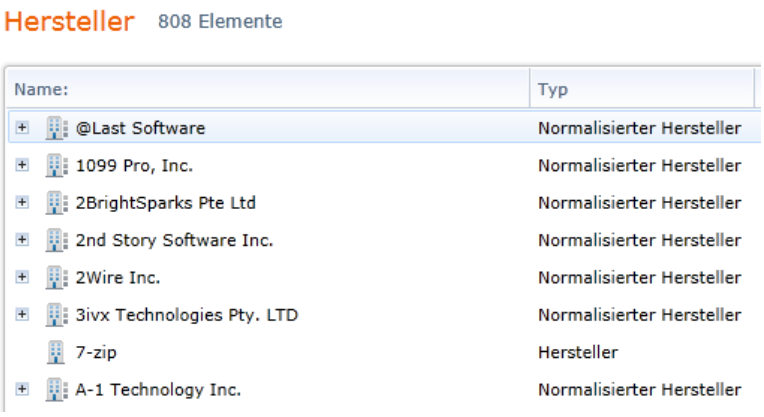
Wenn Sie ein normalisiertes Produkt löschen, sind die von Ihnen ursprünglich mit diesem Produkt verknüpften Lizenzen nicht mehr mit dem Produkt verknüpft. In den Complianceberichten erscheint das normalisierte Produkt dann nicht mehr als ein Produkt, das Lizenzen verbraucht. In diesem Falle sollten Sie die Lizenzen bearbeiten und die Produktverknüpfungen für jede Lizenz überprüfen.

Erstellen eines normalisierten Herstellers

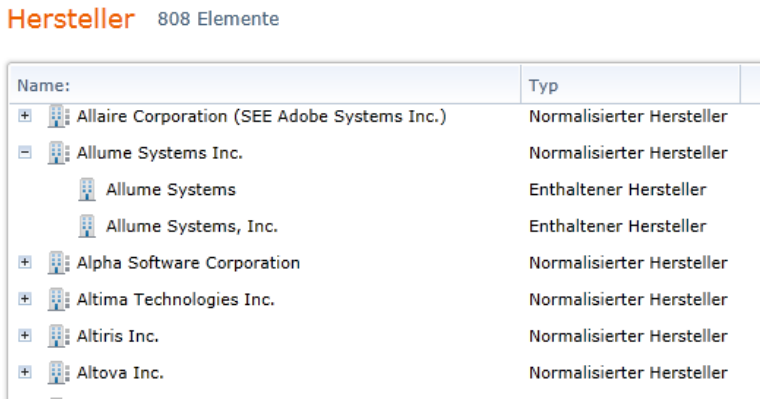
Beim Hinzufügen von Inventardaten zur Softwarelizenzüberwachung werden Sie unter Umständen feststellen, das ein und dasselbe Unternehmen mit verschiedenen Versionen des Unternehmensnamens vertreten ist. Sie können einen normalisierten Herstellernamen erstellen, der anstelle von allen Varianten des Herstellernamens verwendet wird.

Den Namen von normalisierten Herstellern wird in der Liste ein Pluszeichen (+) vorangestellt.

In der folgenden Liste sind beispielsweise vier Varianten des Herstellers Alchemy Software aufgeführt:



Sie können diese Namen auswählen und gruppieren, sodass für alle ein gemeinsamer normalisierter Name verwendet wird. Dieser normalisierte Name wird dann in der Liste angezeigt.



Im Lieferumfang dieses Produkts enthaltene normalisierte Hersteller

Dieses Produkt umfasst normalisierte Hersteller. Wenn Sie die Liste der Hersteller erstmals öffnen, werden Sie feststellen, dass die Liste häufig verwendete Herstellernamen umfasst, die normalisiert wurden.

LANDesk wird eventuell zusätzliche normalisierte Hersteller bereitstellen. Bei Verfügbarkeit werden diese automatisch als Patchinhalte heruntergeladen. Falls Sie bereits selbst normalisierte Hersteller definiert haben sollten, bleibt diese Inhalte erhalten. Auch wenn neue normalisierte Hersteller eventuell mit Ihren eigenen Definitionen in Konflikt stehen sollten, werden Ihre benutzerdefinierten Inhalte keinesfalls von diesen überschreiben.

Definieren eines normalisierten Herstellers

Sie können einen normalisierten Hersteller folgendermaßen definieren.

So erstellen Sie einen normalisierten Hersteller

1. Klicken Sie auf **Administration > Hersteller**.
2. Suchen Sie (ggf. unter Verwendung des Felds **Suchen**) die Herstellernamen, den Sie kombinieren möchten.
3. Wählen Sie die Herstellernamen aus, die in den normalisierten Namen eingeschlossen werden sollen.
4. Klicken Sie auf **Aktionen > Gruppe**.
5. Wählen Sie den Namen aus, den Sie für den normalisierten Hersteller verwenden möchten. (Sie müssen einen der vorhandenen Namen auswählen.)
6. Klicken Sie auf **OK**.

Der von Ihnen gewählte Name wird zu den Namen der normalisierten Hersteller in der Herstellerliste hinzugefügt. Wenn Sie den Namen erweitern (indem Sie auf **+** klicken), werden alle Namen angezeigt, die für diesen normalisierten Namen zusammengruppiert wurden.

So fügen Sie automatisch Hersteller zu einem normalisierten Hersteller hinzu

Sie können Regeln erstellen, mit denen beliebige Herstellernamen automatisch zu einem normalisierten Namen hinzugefügt werden. Sie können beispielsweise angeben, dass alle Herstellernamen, die mit "Adobe Sys*" beginnen, automatisch zum normalisierten Namen "Adobe Systems Incorporated" hinzugefügt werden.

1. Klicken Sie auf **Administration > Hersteller**.
2. Klicken Sie in der Symbolleiste auf **Neu > Hersteller**.

3. Geben Sie einen Namen für den normalisierten Hersteller ein.
4. Klicken Sie auf **Dynamische Regeln**.
5. Geben Sie eine Regel in das Feld ein. Verwenden Sie das Sternchen (*) als Platzhalter in der Suche nach Übereinstimmungen.
6. Um eine weitere Regel hinzuzufügen, klicken Sie auf die Schaltfläche **Hinzufügen** [+] und geben eine weitere Regel ein.
7. Klicken Sie abschließend auf **Speichern**.

Derzeit in der Datenbank enthaltene Herstellernamen, die mit den Regeln übereinstimmen, werden im Feld **Übereinstimmende Hersteller** aufgelistet. Werden nun neue Inventardaten und andere ähnliche Herstellernamen zur Datenbank hinzugefügt, so werden diese Namen automatisch unter dem Namen des normalisierten Hersteller eingeschlossen.

So fügen Sie einen Herstellernamen zu einem vorhandenen normalisierten Hersteller hinzu

Wenn Sie einen normalisierten Hersteller erstellt haben und im Anschluss daran einen weiteren Herstellernamen finden, den Sie zusammen mit den anderen Namen einschließen möchten, können Sie diesen Namen zum normalisierten Namen hinzufügen.

1. Klicken Sie auf **Administration > Hersteller**.
2. Wählen Sie den Herstellernamen aus, den Sie als den Namen des normalisierten Herstellers verwenden möchten.
3. Klicken Sie auf **Aktionen > Zum normalisierten Hersteller verschieben**.
4. Wählen Sie einen normalisierten Hersteller aus und klicken Sie auf **OK**.

Überwachen von Webprodukten

Sie können webgestützte Anwendungen auf dieselbe Art und Weise überwachen, wie Sie Software überwachen, die auf einem Gerät installiert ist. Um diese Art von Produkten in der SLM-Konsole zu überwachen, erstellen Sie Webprodukte.

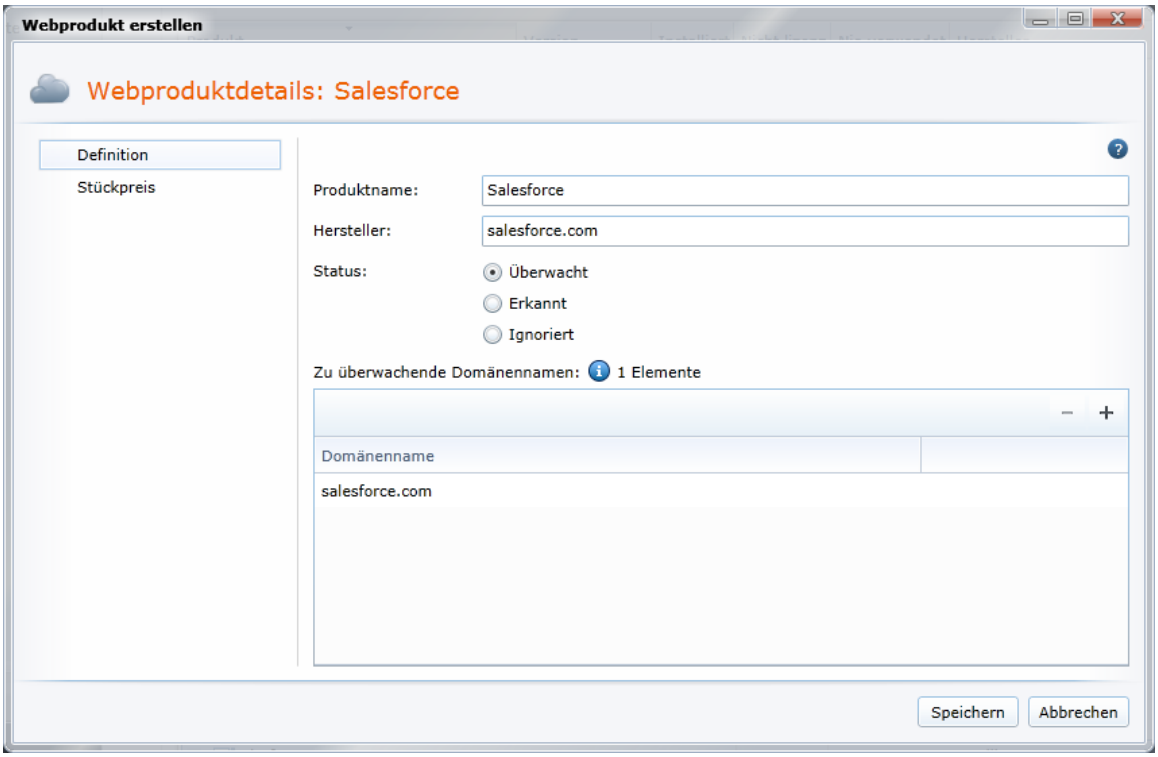
Bei der Erstellung eines Webprodukts in der SLM-Konsole geben Sie die URL an, mit der das Produkt verknüpft ist. Diese URL wird zur Liste der Elemente hinzugefügt, nach denen der Inventarscanner auf verwalteten Geräten sucht. Sie müssen lediglich die Domäne auf der obersten Ebene angeben. Einen Pfad, eine Portnummer oder einen Seitennamen innerhalb der Domäne können Sie nicht angeben. Sie können Unterdomänen hinzufügen.

Der Inventarscanner kann dann verfolgen, welche Geräte auf die URL zugreifen und für welche Dauer. Die entsprechenden Daten werden dann in die Berichte und Berechnungen zur Softwareüberwachung einbezogen.

Wenn Sie beispielsweise Salesforce zur Verfolgung von Vertrieb und Kundendienst verwenden, würden Sie ein Produkt namens "Salesforce" definieren und es mit der URL verknüpfen, auf die zur Anmeldung zugegriffen wird.

Definieren eines Webprodukts

1. Klicken Sie auf **Produkte > Überwacht**.
2. Klicken Sie in der Symbolleiste auf **Neu > Webprodukt**.



3. Geben Sie einen Namen in das Feld **Produktname** ein.
4. Geben Sie mindestens drei Zeichen in das Feld **Hersteller** ein, um Namen mit den entsprechenden Zeichen anzuzeigen. Wählen Sie den Herstellernamen aus. Wenn es keine Übereinstimmung gibt, geben Sie den vollständigen Herstellernamen in das Feld ein.
5. Wählen Sie unter **Status** entweder **Überwacht** oder **Ignoriert** aus, um dieses neue Produkt in einer dieser Produktansichten aufzulisten.
6. Klicken Sie unter **Zu überwachende Domänennamen** auf die Schaltfläche **Hinzufügen (+)**.
7. Geben Sie den Domänennamen für das Webprodukt ein.
8. Klicken Sie auf **Stückpreis**. Wählen Sie ein Verfahren zur Berechnung des Stückpreises aus.
   - Wählen Sie **Automatisch berechneten Stückpreis in allen Berechnungen verwenden**, wenn es mehrere Lizenzen mit unterschiedlichen Stückpreisen für dieses Produkt gibt. Wenn Sie diese Option auswählen, wird als Stückpreis der Durchschnitt aller Stückpreise der verschiedenen Lizenzen verwendet.
   - Wählen Sie **Geben Sie einen Stückpreis an**, wenn Sie denselben Stückpreis in sämtlichen Berechnungen verwenden wollen. Wenn Sie beispielsweise zwei Lizenzen mit unterschiedlichen Preisen für ein und dasselbe Produkt haben und den höheren der beiden Preise in Berechnungen verwenden möchten, können Sie diesen Stückpreis hier angeben.
9. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

Anzeigen aller Geräte, auf denen ein Produkt installiert ist

Wenn Sie sich eine Liste von Produktnamen ansehen oder Diagramme im Dashboard, dann können Sie eine Liste aller Geräte anzeigen, auf denen ein Produkt installiert ist.

Wenn Sie die Liste der Geräte anzeigen, können Sie einen druckbaren Bericht der Liste erstellen oder die Daten zu Referenzzwecken in eine CSV-Datei exportieren.

So zeigen Sie Geräte für ein Produkt in der Produktliste an

1. Klicken Sie auf die Registerkarte **Produkte** und klicken Sie dann auf eine der Produktansichten (Überwacht, Erkannt, Ignoriert oder Alle installierten Produkte).
2. Suchen Sie das Produkt mithilfe des Felds **Suchen** oder mithilfe des Links **Produkte auswählen**.
3. Doppelklicken Sie auf den Produktnamen.

   In einem neuen Fenster wird eine Liste mit Geräten angezeigt.
4. Um eine Liste der Geräte in das CSV-Format zu exportieren, wählen Sie die Geräte aus und klicken Sie dann auf die Schaltfläche **Exportieren** .
5. Um einen Bericht zu den Geräten zu erstellen, klicken Sie auf die Schaltfläche **Bericht** .

So zeigen Sie Geräte für ein Produkt in einem Dashboard-Diagramm an

1. Klicken Sie auf **Dashboard** und wählen Sie dann eine der Dashboard-Optionen (Audits, Compliance oder Lizenzoptimierung) aus.
2. Klicken Sie auf ein Segment des Diagramms, das ein Produkt darstellt.

   Daraufhin wird in einem separaten Fenster ein Liste mit Geräten angezeigt.
3. Um eine Liste der Geräte in das CSV-Format zu exportieren, wählen Sie die Geräte aus und klicken Sie dann auf die Schaltfläche **Exportieren** .
4. Um einen Bericht zu den Geräten zu erstellen, klicken Sie auf die Schaltfläche **Bericht** .

Zurücksetzen der Verwendungsberechnung für ein Produkt

Normalerweise wird die Produktverwendung ab dem ersten Auftreten eines Produkts in einem Inventarscan berechnet. Im Laufe der Zeit können Situationen auftreten, in denen Sie die Berechnung zurücksetzen möchten, um ein genaueres Bild der aktuellen Produktverwendung zu erhalten.

Wenn zum Beispiel ein Produkt für mehrere Monate installiert war und auf manchen Computern einige Male verwendet wurde, können Sie die Berechnung der Produktverwendung für dieses Produkt zurücksetzen. Im Anschluss daran spiegeln die neuen Verwendungsdaten (Anzahl der Starts und Verwendungsdauer in Minuten) lediglich die Nutzung ab dem Zeitpunkt wieder, zu dem die Rücksetzung erfolgt ist.

HINWEIS: Denken Sie daran, dass beim Zurücksetzen der Verwendungsberechnung für ein Produkt alle vorhandenen Produktverwendungsinformationen für dieses Produkt aus der Datenbank entfernt werden.

So setzen Sie die Verwendungsberechnung für ein Produkt zurück

1. Klicken Sie auf die Registerkarte **Produkte** und klicken Sie dann auf eine der Produktansichten (Überwacht, Erkannt oder Alle installierten Produkte).
2. Suchen Sie das Produkt mithilfe des Felds **Suchen** oder mithilfe des Links **Produkte auswählen**.
3. Klicken Sie mit der rechten Maustaste auf das Produkt und wählen Sie **Produktverwendung zurücksetzen**.
4. Klicken Sie auf **Ja** und bestätigen Sie dann, dass Sie die Informationen löschen möchten.

Angeben von Dateien zur Erkennung der Produktinstallation und -verwendung

Es gibt zwei Möglichkeiten, zu erkennen, ob ein Produkt auf einem verwalteten Gerät installiert ist und verwendet wird. Der Inventarscanner identifiziert zwei Arten von Dateien:

- Dateien, die anzeigen, dass das Produkt installiert wurde
- Dateien, die anzeigen, dass das Produkt verwendet wurde

Dateien werden anhand von Dateiname, Versionsnummer und Dateigröße (in Byte) definiert. Automatisch erkannte Produkte werden ebenfalls eindeutig durch die mit dem Produkt verknüpfte GUID identifiziert. Daher kann es so aussehen, als ob es bei einem Produkt Duplikate gibt. Zwei Produkte können einen ähnlichen Namen und eine ähnliche Version, aber unterschiedliche GUIDs aufweisen.

Wenn Sie ein Produkt erstellen oder bearbeiten, können Sie die Definitionen ändern, die für die Erkennung von Dateien verwendet werden. Die nachstehenden Anweisungen gelten für die Bearbeitung eines vorhandenen Produkts.

So geben Sie Dateien zur Erkennung der Produktinstallation oder -verwendung an

1. Klicken Sie auf **Produkte > Überwacht**, um überwachte Produkte anzuzeigen.
2. Klicken Sie auf den Namen eines einzelnen Produkts (nicht auf ein normalisiertes Produkt).
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Bearbeiten**. Das Dialogfeld **Produktdetails** wird aufgerufen. Einige Elemente sind schreibgeschützt, andere können bearbeitet werden.
4. Wählen Sie unter **Status** entweder **Überwacht** oder **Ignoriert** aus, um dieses neue Produkt in einer der Produktansichten aufzulisten.
5. Klicken Sie auf **Installationserkennung**. Beachten Sie, dass alle Optionen schreibgeschützt sind.
6. Klicken Sie auf **Nutzungserkennung**. Sie können Dateien hinzufügen, die darauf hinweisen, dass das Produkt verwendet wird.
7. Klicken Sie auf die Schaltfläche **Hinzufügen (+)**. Im Dialogfeld **Dateien hinzufügen** können Sie entweder einen (in der Inventardatenbank) vorhandenen Dateinamen auswählen oder auf **Neue Datei definieren** klicken und den Dateinamen, die Größe der Datei und die Versionsnummer der Produktdatei eingeben. Wiederholen Sie diese Schritte für alle Produktdateien, die Sie verwenden möchten, um zu bestimmen, ob das Produkt verwendet wird. Klicken Sie abschließend auf **OK**.
8. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

Angeben eines Stückpreises für ein überwachtes Produkt

Die Softwarelizenzüberwachung umfasst mehrere unterschiedliche Berechnungen in Bezug auf die Lizenzverwendung in Ihrem Unternehmen. Das Dashboard "Compliance" beispielsweise enthält eine Schätzung der Kosten, die entstehen, wenn Sie dafür sorgen, dass die Lizenzbedingungen bei allen Produkten erfüllt sind.

Zu jedem überwachten Produkt können Sie die Stückkosten angeben, die in diesen Berechnungen verwendet werden. Die von Ihnen angegebenen Kosten können unter Umständen von den automatisch berechneten Kosten abweichen.

In Fällen, in denen eine Lizenz pro Produkt vorliegt, können Sie die automatische Berechnung verwenden, bei der der Gesamtpreis der Lizenz durch die Anzahl der Lizenzen geteilt wird.

In Fällen, in denen es mehr als eine Lizenz pro Produkt gibt, haben Sie gemäß den Bedingungen der Lizenz unter Umständen andere Stückkosten. Wenn Sie beispielsweise eine Lizenz für eine Version eines Produkts erworben haben und dann eine neue Lizenz für eine neuere Version gekauft haben, dann hat das neuere Produkt eventuell mehr gekostet. Wenn Sie diese Lizenzen sowohl für die ältere als auch für die neuere Version des Produkts verwenden können, müssen Sie entscheiden, welcher Preis den tatsächlichen Kosten entspricht, die Sie in Berechnungen verwenden wollen.

Für die Angabe eines Stückpreises gibt es zwei Optionen:

- **Automatisch berechneten Stückpreis in allen Berechnungen verwenden**: Bei Auswahl dieser Option erfolgen die Berechnungen auf der Basis der Lizenzdaten für das Produkt. Gibt es eine Lizenz für ein Produkt, wird der Stückpreis berechnet, indem die Gesamtkosten durch die Anzahl der Lizenzen geteilt wird. Gibt es mehrere Lizenzen für ein Produkt, errechnet sich der Stückpreis aus dem Durchschnitt der Stückkosten aller Lizenzen für das Produkt (d. h. alle Gesamtkosten dividiert durch die Anzahl aller Lizenzen).
- **Geben Sie einen Stückpreis an, der in sämtlichen Berechnungen verwendet werden soll**: Wenn Sie diese Option auswählen, tritt der von Ihnen eingegeben Preis an die Stelle sämtlicher automatischen Berechnungen. Angenommen, Sie haben für ein Produkt mehrere verschiedene Lizenzen, dann können Sie den aktuellen Preis pro Lizenz angeben, denn diesen Preis müssten Sie beim Kauf einer zusätzlichen Lizenz bezahlen.

Wenn Sie im SLM-Dashboard auf Berechnungen stoßen, die Ihnen fehlerhaft erscheinen, sollten Sie sicherstellen, dass die Kostendaten bei allen Lizenzen für ein Produkt korrekt ausgewiesen sind. Anschließend können Sie entscheiden, ob Sie den Stückpreis für das Produkt dahingehend ändern, dass er die Lizenzkosten für dieses Produkt akkurat wiedergibt.

So geben Sie den Stückpreis für ein Produkt an.

1. Klicken Sie auf **Produkte > Überwacht**, um überwachte Produkte anzuzeigen.
2. Wählen Sie (ggf. unter Verwendung der Felds **Suchen**) das Produkt aus.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Bearbeiten**.
4. Klicken Sie auf **Stückpreis**.
5. Wählen Sie den automatisch berechneten Preis aus oder klicken Sie auf **Geben Sie einen Stückpreis an** und geben Sie in das Feld **Stückpreis** einen Kostenbetrag ein.
6. Klicken Sie auf **Speichern**.

Beachten Sie, dass Sie bei der Auswahl eines normalisierten Produkts sicherstellen sollten, dass die Stückkosten repräsentativ für alle Versionen des Produkts sind, die in das normalisierte Produkt eingeschlossen sind.

Verwenden einer Abfrage zur Bestimmung, wann ein Produkt installiert wurde

Die Mehrzahl der Produkte werden bei Inventarscans anhand von ausführbaren Dateien erkannt, die darauf hinweisen, dass ein Produkt installiert wurde oder verwendet wird. in manchen Fällen können Sie erkennen, dass ein Softwareprodukt auf einem Gerät verwendet wird, indem Sie nach anderen Inventardaten suchen.

Zu diesem Zweck erstellen Sie eine Abfrage in der Management Suite Netzwerkansicht, die auf Inventardaten basiert. Sie können dann auf diese Abfrage als das Element verweisen, das zur Erkennung der Installation verwendet wird, wenn Sie ein benutzerdefiniertes Produkt erstellen.

Ist ein Produkt beispielsweise mit einem Dongle lizenziert ist, der an den Computer angeschlossen werden muss, damit das Produkt verwendet werden kann, dann können Sie eine Abfrage erstellen, die den Dongle als Hardwareinventarelement identifiziert. Wenn der Dongle an einen Computer angeschlossen ist, erkennt der Inventarscanner den Dongle. Wenn Sie diese Abfrage mit dem Produkt verknüpfen, ordnet das Extra "Softwarelizenzüberwachung" diese Daten dem Produkt zu. In den SLM-Berechnungen zeigt das Vorhandensein des Dongles an, wann das Produkt verwendet wird.

Ein weiteres Beispiel wäre eine installierte Schriftart, die pro Computer lizenziert ist. Sie können eine Abfrage mit dem Namen der Schriftart und der Version erstellen und diese Abfrage dann mit der Produktdefinition für die Schriftart verknüpfen. Der Inventarscanner erkennt dann jedwede Nutzung der Schriftart und diese Daten werden in der SLM-Konsole gemeldet.

WICHTIG: Jede Abfrage, die Sie zur Produktidentifikation erstellen, muss die Computer.ID als eine der Abfragekomponenten enthalten. Fehlt die Computer.ID, werden keine Daten für die Abfrage zurückgegeben. Fügen Sie die Komponente zu Ihrer Abfrage hinzu und wählen Sie sie als eine der anzuzeigenden Spalten aus.

So verwenden Sie eine Abfrage zur Erkennung von Produktinstallationen

1. Öffnen Sie in der Management Suite Konsole die Netzwerkansicht und klicken Sie mit der rechten Maustaste auf **Eigene Abfragen**. Wählen Sie **Neue Abfrage** aus. Definieren Sie die Abfrage mit den Elementen, anhand derer das zu überwachende Softwareprodukt identifiziert werden kann und schließen Sie dabei die Computer.ID als eine Komponente ein. Speichern Sie die Abfrage.
2. Klicken Sie auf **Extras > Berichte / Überwachung > Softwarelizenzüberwachung**, um die SLM-Konsole zu öffnen.
3. Klicken Sie auf **Produkte > Überwacht**. Klicken Sie in der Symbolleiste auf **Neu > Benutzerdefiniertes Produkt**.
4. Geben Sie den Produktnamen, die Version und den Herstellernamen ein.
5. Klicken Sie auf **Installationserkennung** und wählen Sie **Abfrageerkennung verwenden** aus.
6. Klicken Sie auf **Durchsuchen**. Suchen Sie unter **Eigene Abfragen** die von Ihnen erstellte Abfrage. Wählen Sie sie aus und klicken Sie anschließend auf **OK**.
7. Fügen Sie weitere Produktdaten auf den Seiten **Nutzungserkennung** und **Stückpreis** hinzu. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

Überwachen der Softwarelizenz-Compliance

Die Softwarelizenz-Compliance bildet eine wichtige Komponente Ihrer Gesamtstrategie für das IT-Assetmanagement. Bei einem Audit Ihres Unternehmens wollen Sie in der Lage sein, die Compliance präzise nachweisen zu können, und wenn Ihr Unternehmen über Richtlinien im Hinblick auf die Softwarenutzung verfügt, kann die Softwarelizenz-Compliance dazu beitragen, die Befolgung dieser Richtlinien durch Ihre Mitarbeiter sicherzustellen.

Die Compliance oder Konformität Ihres Unternehmens mit den Bedingungen Ihrer Softwarelizenzen hängt von Folgendem ab:

- präzisen Inventarscans, die Daten dazu liefern, welche Software erkannt wurde und verwendet wird
- präzisen Daten im Hinblick auf die Lizenzbedingungen der Software, die Sie erworben haben
- der korrekten Verknüpfung von Lizenzen mit Produkten und Computergruppen
- der Abstimmung der Lizenzdaten mit Inventardaten

Der erste Punkt wird durch die Inventarscans von LANDesk Management Suite abgedeckt, die auf verwalteten Geräten in Ihrem Netzwerk ausgeführt werden. Diese Scans umfassen einen Softwareüberwachungsscan, der Softwareinformationen in der Datenbank speichert.

Die im zweiten Punkt genannten Daten müssen aus den von Ihrem Unternehmen verwalteten Lizenzdatensätzen zur Datenbank hinzugefügt werden. Sie können jede Lizenz einzeln eingeben oder Daten aus anderen Quellen importieren, indem Sie die Daten aus einer Excel-Kalkulationstabelle in eine CSV-Datei exportieren und diese Daten dann in die SLM-Konsole importieren.

Der dritte Punkt steht in Abhängigkeit zu den Verknüpfungen, die Sie mit Produkten herstellen, wenn Sie eine Lizenz hinzufügen oder bearbeiten. Wenn Sie Lizenzdaten importieren, stellen Sie bei jeder Lizenz sicher, dass diese mit Produkten verknüpft ist, die durch die Bedingungen dieser Lizenz abgedeckt sind. Wenn Lizenzen auf bestimmte Gruppen innerhalb Ihres Unternehmens beschränkt sind, sollten Sie die Lizenzen darüber hinaus mit Computergruppen für diese Unternehmensgruppen verknüpfen.

Der vierte Punkt schließlich wird vom Extra "Softwarelizenzüberwachung" erfüllt, sobald alle erforderlichen Daten in der Datenbank zur Verfügung stehen. Die Compliance wird jeden Tag bei den regelmäßig für die Datenbank ausgeführten Inventarwartungsläufen berechnet. Der Erfolg der Softwarelizenzüberwachung hängt davon ab, wie präzise Ihre Softwarelizenzdaten sind und wie vollständig die Inventarscans die Geräte in Ihrem Unternehmen tatsächlich abdecken. Ihre Compliance-Ergebnisse hängen ferner davon ab, dass die richtigen Computergruppen definiert und mit den Lizenzen verknüpft sind.

Verwandte Themen

"Sicherstellen der Richtigkeit von Lizenzdaten" auf Seite 351

"Erstellen einer Lizenz" auf Seite 352

"Verknüpfen einer Lizenz mit Produkten" auf Seite 355

Sicherstellen der Richtigkeit von Lizenzdaten

Die Verwaltung von Softwarelizenzen ist ein wichtiger Bestandteil des Finanzmanagements Ihres Unternehmens. Das Extra "Softwarelizenzüberwachung" verwendet Lizenzdaten, um Sie darin zu unterstützen, den Grad der Compliance Ihres Unternehmens mit den Bedingungen Ihrer Lizenzen zu bestimmen. Damit die Complianceberechnungen akkurat ausfallen, müssen Ihnen korrekte Lizenzdaten vorliegen.

Am Besten fangen Sie mit einer kleinen Anzahl von Lizenzen an, beispielsweise mit den Lizenzen, die für Audits überwacht werden müssen. Sie können diese Lizenzdaten unter Verwendung der Softwarelizenzüberwachungs-Konsole manuell hinzufügen oder importieren. Die Daten werden dann zum Generieren von Statistiken und Berichten verwendet, mit deren Hilfe Sie herausfinden können, ob Ihre Produktlizenzen im Einklang mit den tatsächlichen Produktinstallationen stehen.

Nach dem Hinzufügen der Lizenzdaten sollten Sie die zur jeder Lizenz gehörigen Produktinformationen überprüfen. Suchen Sie die zu einer Lizenz gehörenden Produkte in der Produktansicht **Erkannt** und verschieben Sie diese in die Ansicht **Überwacht**. Kombinieren Sie gegebenenfalls die verschiedenen Versionen eines Produkts in ein normalisiertes Produkt, um die Verwaltung dieses Produkts in den SLM-Konsole zu vereinfachen.

Mit den folgenden Tasks können Sie die Korrektheit der Lizenzdaten für Ihr Unternehmen sicherstellen:

- Erstellen von Softwarelizenzdatensätzen
- Importieren von Softwarelizenzdaten
- Erstellen von normalisierten Produkten
- Verknüpfen von Softwarelizenzen mit installierten Produkten
- Anzeigen der Softwarelizenz-Compliance
- Neuberechnen der Softwarelizenz-Compliance

Erstellen einer Lizenz

Wenn Ihre Lizenzdaten nicht in einem Format vorliegen, das einfach zu importieren ist, können Sie die Daten manuell in der Ansicht "Lizenzen" eingeben. Die von Ihnen eingegebenen Daten werden in der Datenbank gespeichert und zur Berechnung der Compliance verwendet.

So erstellen Sie eine Lizenz

1. Klicken Sie auf **Produkte > Lizenzen**.
2. Klicken Sie in der Symbolleiste auf **Neu > Lizenz**.
3. Geben Sie auf den drei Seiten des Dialogfelds **Lizenz erstellen** (**Definition**, **Verknüpfte Produkte** und **Datensätze**) Daten ein.
4. Klicken Sie auf **Speichern**, wenn Sie fertig sind.

Klicken Sie hier, um eine Beschreibung der Felder im Dialogfeld **Lizenz erstellen** anzuzeigen.

Seite "Definition"

- **Lizenzname**: Der Name der Lizenz, der unter Umständen dem Produktnamen entspricht.
- **Lizenzmenge**: Die Anzahl der laut Kaufvertrag erlaubten Lizenzen.
- **Stückpreis:** Der für den Erwerb der Lizenz bezahlte Preis.
- **Computergruppe**: Wenn die Lizenz für eine bestimmte Gruppe von Computern erworben wurde, können Sie die Gruppe hier auswählen Diese Gruppe muss in der Ansicht **Computergruppen** der SLM-Konsole vorhanden und damit in der Management Suite Netzwerkansicht erstellt worden sein. Wählen Sie **Alle**, wenn die Lizenz für jeden Computer in Ihrer Organisation verwendet werden kann. Sollte die gewünschte Gruppe nicht in der Liste enthalten sein, klicken Sie auf **Computergruppe erstellen**, um eine neue Gruppe über eine Management Suite-Abfrage oder -Gerätegruppe zu erstellen.
- **Anbieter**: Der Anbieter, von dem Sie die Lizenz erworben haben. Dieser kann gleichzeitig auch der Hersteller sein. Nachdem Sie mindestens drei Zeichen eingegeben haben, werden alle in der Datenbank enthaltenen Anbieternamen mit den entsprechenden Zeichen angezeigt. Wenn einer dieser Namen dem gesuchten Anbieter entspricht, wählen Sie ihn aus der Liste aus.
- **Kaufdatum**: Das Datum, an dem die Lizenz erworben wurde und ab dem sie gültig ist. Klicken Sie auf das Kalendersymbol, um das Datum auszuwählen oder geben Sie das Datum in das Textfeld ein (es wird gemäß Ihrem Standardzahlenformat formatiert, z. B. TT.MM.JJJJ).
- **Ablaufdatum**: Das Datum, an dem die Lizenz abläuft. Dieses Datum ist wichtig, wenn Sie Lizenzen verfolgen wollen, die erneuert werden müssen. Klicken Sie auf das Kalendersymbol, um das Datum auszuwählen oder geben Sie das Datum in das Textfeld ein (es wird gemäß Ihrem Standardzahlenformat formatiert, z. B. TT.MM.JJJJ).
- **Verbrauch**: Die zur Berechnung der Lizenznutzung verwendete Methode.

    - **Eine pro Computer**: Die Lizenznutzung wird je Computer ermittelt, auf dem die Software installiert ist, unabhängig davon, wie viele zusätzliche Installationen auf diesem Computer vorliegen.
- **Compliancetyp**: Der Lizenztyp im Sinne der Lizenzcompliance, wie sie vom Hersteller spezifiziert wurde.
    - **Berechnet**: Die Lizenznutzung wird berechnet, damit die Compliance mit den Verkaufsbedingungen sichergestellt ist. Dies kann folgende Lizenztypen umfassen: Neues Produkt, Kostengünstiges Upgrade, OEM-Lizenz, Produktupgrade, Volumenlizenz, Enterprise Agreement oder Unbekannt.
    - **Nicht berechnet**: Die Lizenznutzung muss nicht berechnet werden, damit Compliance gegeben ist. Dies kann folgende Lizenztypen umfassen: Freeware, Public Domain, Shareware, Floating-Lizenz und Standortlizenz.

Seite "Verknüpfte Produkte"

Diese Seite listet alle Produkte auf, die mit der Lizenz verknüpft sind. Es werden alle Produkte aufgelistet, die laut den Lizenzbedingungen verwendet werden können.

Listen Sie die Produkte in der Reihenfolge auf, in der diese die Lizenzen verbrauchen sollen. Das erste Produkt verbraucht die verfügbaren Lizenzen zuerst. Wenn weitere Lizenzen verfügbar sind, dann verbraucht das zweite Produkt die verfügbaren Lizenzen. Dies setzt sich in der Reihenfolge der Liste fort, bis keine Lizenzen mehr verfügbar sind.

Sie können jedes Produkt mit einer Lizenz verknüpfen. Wenn das Produkt derzeit nicht überwacht wird, verschiebt SLM das Produkt in die Liste **Überwacht**, wenn Sie es mit einer Lizenz verknüpfen.

So fügen Sie verknüpfte Produkte zur Liste hinzu

1. Klicken Sie auf die Schaltfläche **Hinzufügen (+)**.
2. Geben Sie im Dialogfeld **Produkte zur Lizenz hinzufügen** mindestens drei Zeichen in das Feld **Produktname enthält** ein, um die gewünschten Produkte zu finden. Als Ergebnisse werden alle Produkte aufgelistet, die die von Ihnen eingegebene Zeichenfolge enthalten.
3. Um die Ergebnisliste zu filtern, können Sie eine Zeichenfolge in das Feld **Produktname enthält nicht** eingeben. Produkte mit dieser Zeichenfolge werden aus der Liste entfernt. Sie können mehrere Zeichenfolgen verwenden, die durch Leerzeichen voneinander getrennt sind.
4. Um die Anzahl der Ergebnisse in der Produktansicht **Überwacht** zu begrenzen, wählen Sie **Nur überwachte Produkte anzeigen** aus.
5. Wählen Sie ein oder mehrere Produkte aus der Liste der Ergebnisse aus und klicken Sie auf **OK**.

   Die Produkte werden zur Liste **Verknüpfte Produkte** hinzugefügt.
6. Mit den Schaltflächen Pfeil-nach-oben und Pfeil-nach-unten können Sie Produkte in der Liste nach oben oder nach unten verschieben.

Verwandte Themen

"Verknüpfen einer Lizenz mit Produkten" auf Seite 355

Seite "Datensätze"

Diese Seite enthält Daten und Notationen, die die Lizenz in Übereinstimmung mit den Einkaufs- oder Rechnunglegungspratiken Ihres Unternehmens dokumentiert. Diese Informationen werden nicht bei der Lizenzüberwachung verwendet, sind aber für Sie nützlich, wenn darum geht, stets akkurate Aufzeichnungen für Auditzwecke parat zu haben.

- **Hersteller-Rechnungsnummer**: Die vom Softwarehersteller vergebene Rechnungsnummer. Diese Nummer ist für die Verfolgung der Software innerhalb Ihres Einkaufsprozesses wichtig.
- **Bestellungsnummer**: Die Bestellungsnummer, die in Ihrer Organisation beim Erwerb der Software verwendet wurde. Diese Nummer ist für die Verfolgung der Software innerhalb Ihres Einkaufsprozesses wichtig.
- **Lizenzschlüssel**: Der vom Hersteller zur Aktivierung der Lizenz bereitgestellte Schlüssel.
- **Seriennummer**: Die Seriennummer des Herstellers, die mit dieser Lizenz verknüpft ist.
- **Ort**: Ein Vermerk, der Ihnen bei der Bestimmung hilft, wo die Lizenzen in Ihrer Organisation verwendet werden.
- **Unterstützende Dokumente**: Ein Vermerk, der Aufschluss darüber gibt, welche unterstützende Dokumente zu Ihren Lizenzassets vorhanden sind. Dies kann entweder ein Speicherort auf dem Netzwerk oder eine URL oder eine beliebige Beschreibung sein, die Sie verwenden möchten.
- **Notizen**: Geben Sie hier zusätzliche Notizen zu der Lizenz ein. Dieser Notizen werden in der Datenbank gespeichert.

Importieren von Lizenzdaten aus einer CSV-Datei

Sie können vorhandene Lizenzdaten aus einer älteren Version von LANDesk Management Suite oder aus anderen Datenquellen importieren. Die Daten müssen als CSV-Datei gespeichert werden.

Ein Beispiel für eine CSV-Datei (ImportLicense.csv) finden Sie in der LDMAIN-Freigabe des Coreservers (im Ordner LDMAIN\LANDesk\SAM). Beachten Sie die folgenden Richtlinien für die Erstellung einer CSV-Datei für den Import von Lizenzdaten:

- Die einzige erforderliche Spalte in der CSV-Datei ist die Spalte "Name".
- Wenn Sie nicht wissen, was Sie in eine Spalte eingeben sollen, lassen Sie sie leer. Beim Importvorgang wird in jede leere Spalte ein Standardwert eingefügt.
- Nach den Spalten für die Lizenzeigenschaften kommen Spalten für verknüpfte Produkte. Diese tragen die Bezeichnungen "Verknüpftes Produkt 1" und "Produkt 1 Version", "Verknüpftes Produkt 2" und "Produkt 2 Version" und so weiter. Geben Sie den Produktnamen in die Spalte "Verknüpftes Produkt x" ein und die Produktversion in die Spalte "Produkt x Version" Gibt es keine Produktversion, lassen Sie die Spalte leer. Der Importvorgang sucht nach übereinstimmenden Produkten mit dem angegebenen Produktnamen und der angegebenen Version. Werden mehrere Produkte mit demselben Namen und derselben Version gefunden, werden alle übereinstimmenden Produkte mit der Lizenz verknüpft. Mit einer Lizenz kann eine beliebige Anzahl von Produkten verknüpft werden.
- Der Importvorgang überschreibt *keine* vorhandene Lizenzen. Sollte der Name einer vorhandene Lizenz mit dem Namen einer in den Importdaten enthaltenen Lizenz übereinstimmen, wird eine neue Lizenz mit dem Namen "<Lizenzname> [1]" erstellt. Die Zahl in Klammern wird bei jeder weiteren Übereinstimmung um 1 erhöht, sodass jede Lizenz einen eindeutigen Namen erhält.

So importieren Sie Lizenzdaten

1. Erstellen Sie gemäß den oben aufgeführten Richtlinien eine CSV-Datei mit den Lizenzdaten, die Sie importieren möchten.
2. Klicken Sie in der SLM-Konsole auf **Produkte > Lizenzen**. Klicken Sie in der Symbolleiste auf **Aktionen > Aus CSV-Datei importieren**.
3. Navigieren Sie zum Speicherort der CSV-Datei und klicken Sie auf **Öffnen**.

   Die Lizenzdaten werden zur Datenbank hinzugefügt und in der Ansicht **Lizenzen** der Softwarelizenzüberwachungs-Konsole angezeigt.

4. Wenn Sie die importierten Lizenzen überprüfen und die Daten bearbeiten möchten, wählen Sie in der Ansicht **Lizenzen** eine Lizenz aus und klicken Sie auf die Schaltfläche **Bearbeiten**. Überprüfen Sie die Daten auf allen drei Seiten des Dialogfelds ("Definition", "Verknüpfte Produkte" und "Datensätze"). Klicken Sie auf **Speichern**, wenn Sie fertig sind.

Verknüpfen einer Lizenz mit Produkten

Wenn Sie eine Lizenz hinzufügen oder bearbeiten, müssen Sie die Lizenz mit einem oder mehreren Produkten verknüpfen, um die Compliance für die Produktverwendung und die Lizenz zu berechnen Sie können ein oder mehrere Produkte auswählen und auch normalisierte Produkte, die mehrere einzelne Produkte darstellen. Wenn ein Produkt derzeit nicht überwacht wird, verschiebt SLM das Produkt in die Liste **Überwacht**, wenn Sie es mit einer Lizenz verknüpfen.

Wenn Sie verknüpfte Produkte auswählen, listen Sie die Produkte in der Reihenfolge auf, in der diese die Lizenzen verbrauchen sollen. Das erste Produkt verbraucht die verfügbaren Lizenzen zuerst. Wenn weitere Lizenzen verfügbar sind, dann verbraucht das zweite Produkt die verfügbaren Lizenzen. Dies setzt sich in der Reihenfolge der Liste fort, bis keine Lizenzen mehr verfügbar sind.

Nachstehend ist ein Beispiel gegeben, wie die Lizenzberechnung bei mehreren Produktversionen erfolgt.

- Sie haben eine Lizenz für das Produkt ABC erworben, das 30 Installationen (oder Lizenzplätze) zulässt.
- Die Lizenz kann für die Versionen 3, 4 und 5 des Produkts verwendet werden.
- In der Liste Verknüpfte Produkte haben Sie die Versionen so sortiert, dass die neuste Version (5) an erster Stelle steht, gefolgt von der Version 4 und schließlich der Version 3.

In diesem Fall wird die Lizenznutzung wie folgt berechnet:

- 16 Benutzer haben Version 5 installiert, d. h. jeder der 16 verbraucht einen Lizenzplatz.
- 21 Benutzer haben Version 4 installiert; 14 davon verbrauchen einen Lizenzplatz und 7 sind nicht lizenziert.
- 8 Benutzer haben Version 3 installiert sein; keine dieser Installationen ist lizenziert.

Ihre Lizenzcompliance-Berichte zu diesem Produkt werden aufzeigen, dass die Nutzung des Produkts in 15 Fällen nicht durch eine Lizenz abgedeckt ist. Sie müssen dann entscheiden, ob zusätzliche Lizenzen angeschafft werden. Vielleicht überprüfen Sie aber auch die tatsächliche Verwendung der Produkte in Ihrem Unternehmen. Wenn einige Benutzer, die das Produkt\ installiert haben, das Produkt lange Zeit nicht verwendet haben, können Sie nachfragen, ob sie die Software tatsächlich benötigen. Wenn nicht, können diese Benutzer das Produkt deinstallieren und die Lizenzen können für andere Benutzer eingesetzt werden.

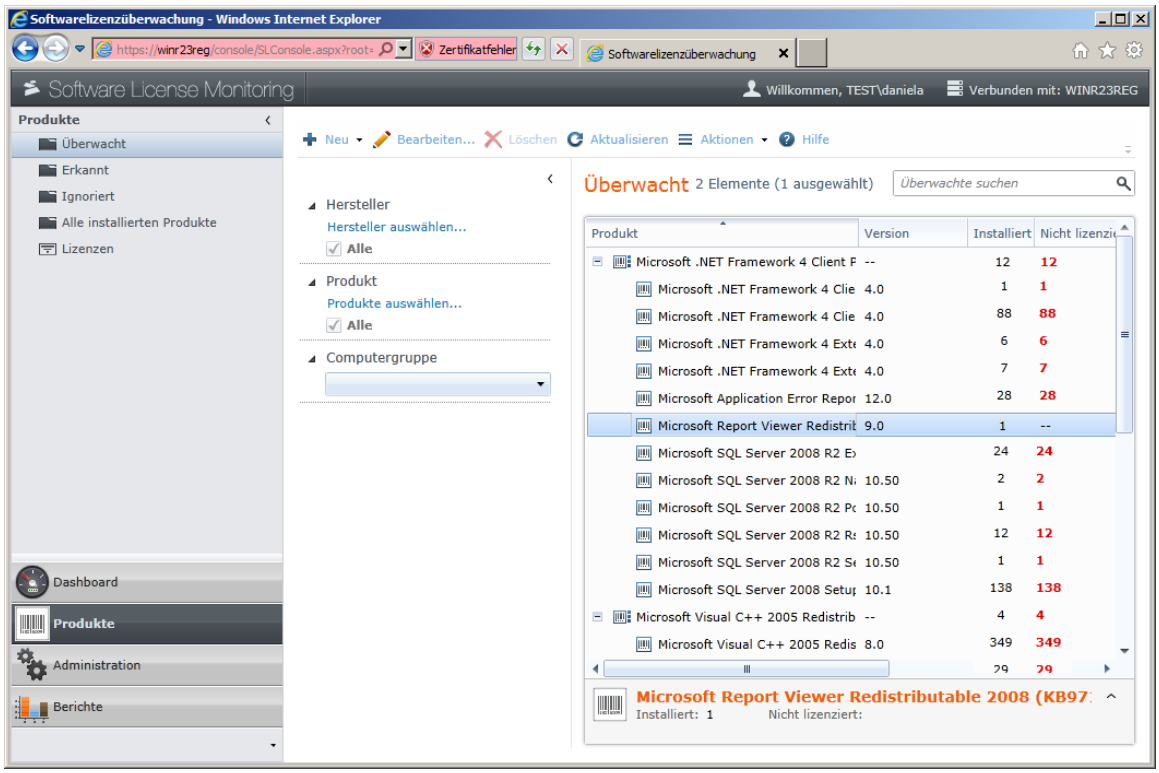
HINWEIS: Lizenzen werden zum Zwecke der Compliancеberechnungen mit Produkten verknüpft. Wenn Sie ein Produkt löschen, ist die von Ihnen mit diesem Produkt verknüpfte Lizenz nicht mehr mit dem Produkt verknüpft. In den Complianceberichten erscheint dieses Produkt dann nicht mehr als ein Produkt, das Lizenzen verbraucht.

Anzeigen von Lizenzcompliancedaten

In der SLM-Konsole gibt es drei verschiedene Wege herauszufinden, ob Ihre Produktinstallationen mit den Bedingungen Ihrer Softwarelizenzen konform sind. In diesem Thema wird beschrieben, wie Sie die hierfür erforderlichen Daten finden.

Anzeigen von Informationen nach Produkt

Öffnen Sie die Produktansicht **Überwacht**, um Informationen zu den in Ihrem Unternehmen installierten Produkten abzurufen. Sie müssen ein Produkt in die Ansicht **Überwacht** verschieben, um möglichst viele Informationen über seine Verwendung und Lizenzierung zu erhalten.



Sie können die folgenden Elemente anzeigen:

- **Produktinstallationen**: Doppelklicken Sie auf den Produktnamen, um eine Liste der Geräte anzuzeigen, auf denen das Produkt installiert ist.
- **Ob es derzeit verwendet wird**: Sehen Sie sich in der Ansicht **Übersicht** die Spalten **Nie verwendet** und **Neunzig Tage seit letzter Verwendung an**, um herauszufinden, ob es Benutzer gibt, die das Produkt gar nicht oder nur sehr selten verwenden.

- **Ob es ordnungsgemäß lizenziert ist**: Vergleichen Sie in der Ansicht **Überwacht** die Spalten **Installiert** und **Nicht lizenziert**, um herauszufinden, ob mehr installierte Exemplare als Lizenzen vorhanden sind.
- **Mit dem Produkt verknüpfte Lizenzen**: Klicken Sie mit der rechten Maustaste und wählen Sie **Lizenzen anzeigen, die dem ausgewählten Produkt entsprechen**, um eine Liste der Lizenzen anzuzeigen, die mit dem Produkt verknüpft sind.

HINWEIS: Sie werden feststellen, dass die Produktansichten **Erkannt** und **Ignoriert** zwar dieselben Spalten aufweisen und allem Anschein nach Compliancedaten zeigen. Diese Daten spiegeln jedoch nicht akkurat die Lizenzen verglichen mit den tatsächlichen Produktinstallationen wider. Nur Produkte in der Produktansicht **Überwacht**, die mit Lizenzen verknüpft sind, zeigen nützliche und akkurate Daten.

Anzeigen von Übersichtsdaten zur Compliance

Die Dashboards enthalten Übersichtsdaten in Bezug auf die Lizenzcompliance und Lizenzoptimierung. Diese Seiten sollen Sie darin unterstützen, die wichtigsten Probleme im Hinblick auf die Softwarelizenzierung anzugehen. Sie können Ihnen zwar kein vollständiges Bild liefern, helfen Ihnen aber, die Probleme zu finden, die zuerst gelöst werden sollten, damit Sie Kosten senken und eine möglichst effiziente Softwarenutzung erreichen.

- **Dashboard "Audits"**: Diese Seite bietet Berichte, die sich bei der Vorbereitung auf ein Audit Ihrer Softwarelizenznutzung als nützlich erweisen.
- **Dashboard "Compliance"**: Diese Seite bietet Berichte, die Aufschluss über Produkte gibt, bei denen die Lizenzcompliance verletzt ist und die Ihre Aufmerksamkeit erfordern.
- **Dashboard "Lizenzoptimierung"**: Diese Seite bietet Berichte mit Schätzwerten für Einsparungen, die durch das Entfernen nicht verwendeter Lizenzen von Computern in Ihrem Unternehmen erzielt werden können.

Anzeigen von lizenzbezogenen Berichten

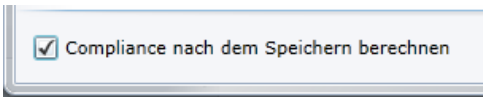
In SLM-Berichten werden Berichtsdaten zu vielen Aspekten Ihre Softwarelizenz-Compliance und -Nutzung zusammengeführt. Anhand von Berichten können Sie alle Details zu einem bestimmten Problem oder Bedarf finden und die Daten dann exportieren oder den Bericht per E-Mail an Dritte schicken, damit diese tätig werden können.

- **Berichte für Audits**: Diese Berichte erweisen sich bei der Vorbereitung auf ein Audit Ihrer Softwarelizenznutzung als nützlich. Sie umfassen Auditkennzeichen, beispielsweise überwachte Produkte ohne verknüpfte Lizenzen und Lizenzen ohne unterstützende Daten wie Rechnungs- oder Bestellungsnummern.
- **Berichte zur Compliance**: Diese Berichte enthalten Details zu allen Produkten und Lizenzen, bei denen keine Compliance gegeben ist. Hierzu gehört ein Überblick über den Lizenzverbrauch für sämtliche Produkte sowie die Gesamtkosten, um für alle Produkten Compliance zu erreichen.
- **Berichte zur Lizenzoptimierung**: Diese Berichte bieten Details, die Sie darin unterstützen, die Softwarenutzung in Ihrem Unternehmen zu optimieren. Sie umfassen Listen nicht verwendeter Softwarelizenzen, nicht oder nur selten verwendeter Produkte sowie andere damit in Zusammenhang stehende Daten.

Neuberechnung der Lizenzcompliance

Die Lizenzcompliance wird auf täglicher Basis immer dann berechnet, wenn ein Inventarwartungslauf für Ihre Datenbank stattfindet.

Bei vielen Tasks im Zusammenhang mit Produkten und Lizenzen wird eine Neuberechnung durchgeführt, sobald Sie die Daten speichern, die Sie geändert haben. Wenn Sie ein Kontrollkästchen mit der Bezeichnung **Compliance nach dem Speichern berechnen** sehen, weist dies darauf hin, dass die Berechnung der Lizenzcompliance im Anschluss an die Speicherung Ihrer Arbeit erneut ausgeführt wird.

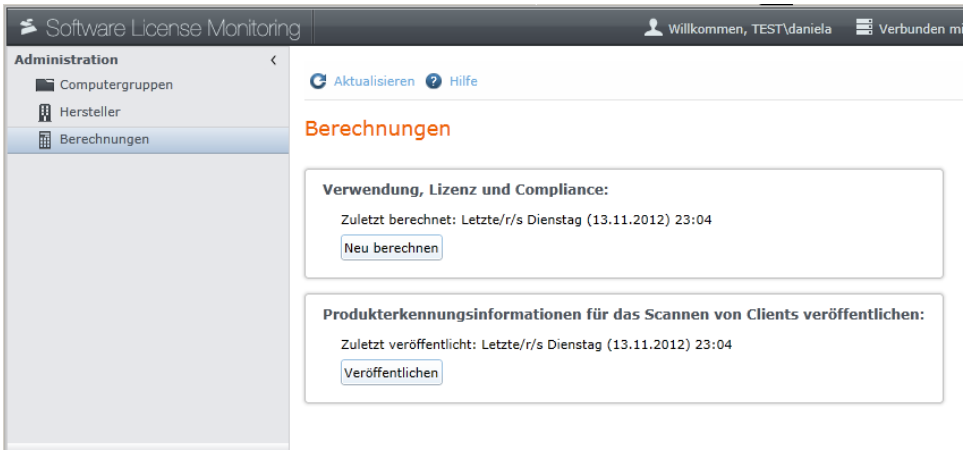


Wenn Sie Lizenzdaten hinzugefügt oder andere Änderungen vorgenommen haben und die Compliance neu berechnen möchten, ohne hierfür die geplante Wartung abwarten zu müssen, können Sie die Neuberechnung der Produktverwendung und der Lizenzcompliance veranlassen.

Eine entsprechende Option gibt Ihnen die Möglichkeit, neue Produkterkennungsinformationen zu der Inventarscandatei hinzuzufügen, die zur Erkennung von installierten Produkten bzw. verwendeten Produkten dient. Wenn Sie die Installation oder Verwendung des Produkts durch Angabe der Dateien zur Identifizierung des Produkts definiert haben, können Sie diese Informationen veröffentlichen, so dass sie verfügbar sind, wenn das nächste Mal ein Inventarscan für verwaltete Geräte durchgeführt wird.

So berechnen Sie die Verwendung und die Compliance neu

1. Klicken Sie auf **Administration > Berechnungen**.



2. Zur Aktualisierung der Verwendung und der Lizenzcompliance klicken Sie auf die Schaltfläche **Neu berechnen**.
3. Zur Veröffentlichung neuer Produkterkennungsinformationen, die bei Clientinventarscans zum Einsatz kommen, klicken Sie auf die Schaltfläche **Veröffentlichen**.

Erstellen eines Berichts mit Softwarelizenzüberwachungsdaten

Das Extra LANDesk Management Suite Berichte kann in Verbindung mit der Softwarelizenzüberwachungs-Konsole verwendet werden. Sie können damit einen druckbaren Bericht zu den Daten erstellen, die gegenwärtig in der Konsole angezeigt werden.

Wenn Sie einen Bericht zur aktuellen Ansicht erstellen, umfasst der Bericht sämtliche derzeit aufgelisteten Elemente. Die Daten werden nach denselben Spalten organisiert, die in der aktuellen Ansicht angezeigt werden. Sie können den Bericht in sechs verschiedenen Formaten speichern.

Ferner können Sie vordefinierte Berichte ausführen, die mit der Berichtsfunktion bereitgestellt werden. Diese Berichte sind in der SLM-Konsole auf der Seite **Berichte** aufgeführt.

WICHTIG: Wenn Sie Internet Explorer 9 für die SLM-Konsole verwenden, müssen Sie die Kompatibilitätsansicht einschalten, um die Management Suite Berichte anzeigen zu können. Um die Kompatibilitätsansicht einzuschalten, öffnen Sie Internet Explorer 9. Drücken Sie die **Alt**-Taste, um das Menü anzuzeigen und klicken Sie dann auf **Extras > Kompatibilitätseinstellungen**. Markieren Sie das Kontrollkästchen **Alle Websites in Kompatibilitätsansicht anzeigen** und klicken Sie auf **Schließen**.

So erstellen Sie einen Bericht zu Daten in Konsole

1. Zeigen Sie in der SLM-Konsole beliebige Produkt- oder Lizenzdaten an.
2. Klicken Sie in der Symbolleiste auf **Aktionen > Druckbarer Bericht zu den Suchergebnissen**.

   Der Bericht wird in einem separaten Berichts-Viewer-Fenster geöffnet.
3. Wählen in der Symbolleiste des Bericht-Viewers ein Berichtsformat aus.
4. Wenn Sie eine Kopie des Berichts speichern möchten, klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren**.
5. Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort für die Datei aus. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Exportieren**, um den Bericht zu speichern.

Auf manchen Seiten gibt es eine Schaltfläche **Bericht**, die Sie anstelle der Symbolleiste im Schritt 2 verwenden können.

So führen Sie einen vordefinierten Bericht aus

1. Klicken Sie in der SLM-Konsole auf **Berichte**.
2. Klicken Sie auf **Berichte > Standardberichte > Softwarelizenzüberwachung** und suchen Sie den gewünschten Bericht.
3. Wählen Sie den Bericht aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Bericht ausführen**.

   Der Bericht wird in einem separaten Berichts-Viewer-Fenster geöffnet.
4. Wählen in der Symbolleiste des Bericht-Viewers ein Berichtsformat aus.

5. Wenn Sie eine Kopie des Berichts speichern möchten, klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren** .
6. Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort für die Datei aus. Klicken Sie auf **Speichern**, und klicken Sie dann auf **Exportieren**, um den Bericht zu speichern.

Definieren einer Computergruppe

Bei der Überwachung der Software- und Lizenznutzung ist es unter Umständen wünschenswert, Gruppen von Computern mit Lizenzen zu verknüpfen. Eine Gruppe kann beispielsweise die Computer an einem bestimmten Standort oder innerhalb eines Geschäftsbereichs Ihres Unternehmens mit eigener Kontoführung für Softwarelizenzen darstellen.

Lizenzen können auf zweierlei Arten mit Gruppen verknüpft werden:

- **Statische Gruppe**: Dies ist eine Gruppe von Computern, die Sie in der Management Suite Netzwerkansicht ausgewählt und als Gerätegruppe gespeichert haben.
- **Dynamische Gruppe**: Dies ist eine Gruppe von Computern, die über eine Abfrage in der Management Suite Netzwerkansicht definiert ist. Wenn überwachte Geräte hinzugefügt oder entfernt werden, ändert sich der Inhalt der Gruppe so, dass er den Parametern der Abfrage entspricht.

Gruppen können nur in der Management Suite Netzwerkansicht erstellt werden. Wenn Sie eine Gruppe in der SLM-Konsole definieren, wählen Sie einfach einen Namen, der mit einer bereits vorhandenen Gerätegruppe oder Abfrage verknüpft werden soll.

So definieren Sie eine Computergruppe

1. Klicken Sie auf **Administration > Computergruppen**.
2. Klicken Sie in der Symbolleiste auf **Neu > Computergruppe**.
3. Geben Sie einen Namen für die Gruppe ein. Dieser Name dient zur Identifizierung der Gruppe in der SLM-Konsole.
4. Erweitern Sie **Geräte** oder **Abfragen** und suchen Sie die Gerätegruppe bzw. die Abfrage, die den Ursprung der Computer darstellt.
5. Wenn alle Informationen vollständig sind, klicken Sie auf **Speichern**.

So löschen Sie eine Computergruppe

1. Klicken Sie auf **Administration > Computergruppen**.
2. Wählen Sie in der Liste eine Gruppe aus. Klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen**.
3. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

HINWEIS: Wenn Sie eine Computergruppe löschen, sind alle damit verknüpften Lizenzen nicht mehr mit den betreffenden Computern verknüpft, d. h. die Complianceberichte sind für diese Gruppe nicht anwendbar. Wenn Sie dies tun, müssen Sie entscheiden, welche Computer mit der betreffenden Lizenz verknüpft werden sollen und eine neue Gruppe definieren. Wenn keine Verknüpfung mit einer Gruppe besteht, wird die Lizenz mit allen Computern verknüpft.

Anzeigen der installierten Produkte für eine Computergruppe

Anfänglich befinden sich sämtliche Produkte, die auf allen Computern in Ihrer Inventardatenbank erkannt wurden, in der Produktgruppe **Erkannt**. Dies ergibt sehr schnell eine große Anzahl von Datensätzen. Verschieben Sie daher Produkte in die Produktansichten **Überwacht** oder **Ignoriert**, um diejenigen Produkte zu identifizieren, die Sie aktiv überwachen wollen bzw. diejenigen, die Sie nicht überwachen wollen.

Wenn Sie Computergruppen definieren, haben Sie die Möglichkeit, nur die Software anzuzeigen, die auf einer bestimmten Gruppe von Computern installiert ist. Eine kleinere Gruppe von Produktdatensätzen für ausgewählte Computer kann so auf einfache Weise angezeigt werden.

So zeigen Sie die installierten Produkte für eine Computergruppe an

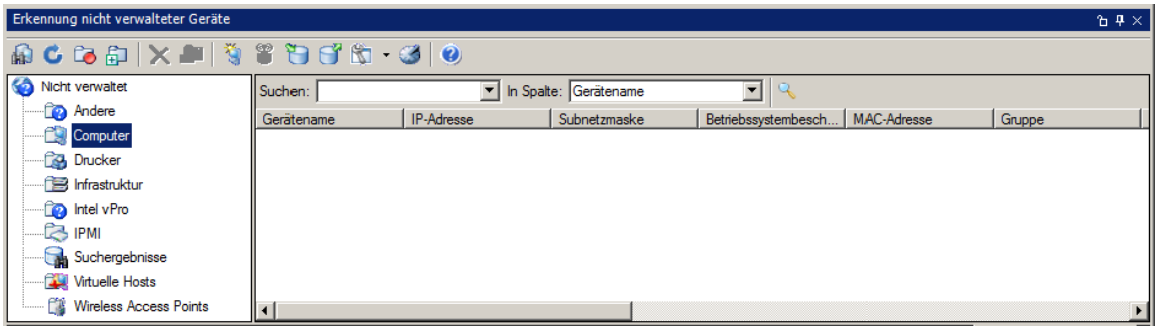
1. Klicken Sie auf **Produkte** und wählen Sie **Überwacht**, **Erkannt**, **Ignoriert** oder **Alle installierten Produkte** aus.
2. Wählen Sie unter **Computergruppe** eine Computergruppe aus der Liste aus.

Die Liste der Produkte ändert sich dahingehend, dass nur Produkte angezeigt werden, die auf den Computern in der von Ihnen ausgewählten Gruppe installiert sind.

Erkennung nicht verwalteter Geräte

Erkennung nicht verwalteter Geräte – Übersicht

Die Erkennung nicht verwalteter Geräte (UDD, Unmanaged Device Discovery) bietet viele Möglichkeiten, nicht verwaltete Geräte in Ihrem Netzwerk zu scannen und zu erkennen.



Hier sind die grundlegenden UDD-Scanmethoden aufgeführt:

- **Netzwerkscan:** Sucht mithilfe einer ICMP-Ping-Suche nach Computern. Diese Suche ist am gründlichsten, verursacht jedoch auch den größten Zeitaufwand. Sie können die Suche auf bestimmte IP- und Subnetzbereiche beschränken. Standardmäßig verwendet diese Option NetBIOS, um Informationen über das Gerät zu sammeln.
    - **IP-Betriebssystem-Fingerabdruck:** Verwenden Sie nmap, wenn Sie versuchen möchten, weitere Informationen zu einem Gerät zu sammeln, wie beispielsweise den Betriebssystemtyp, der darauf ausgeführt wird.
    - **SNMP:** UDD verwendet SNMP zum Erkennen von Geräten. Klicken Sie auf **Konfigurieren**, um Informationen zu SNMP in Ihrem Netzwerk einzugeben.
- **Standard LANDesk Agent:** Sucht auf Computern nach dem Standard LANDesk Agenten (CBA). Diese Option erkennt Geräte, auf denen LANDesk Produkte installiert sind.
- **NT-Domäne:** Sucht in einer von Ihnen angegebenen Domäne nach Geräten. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.
- **LDAP:** Sucht in einem von Ihnen angegebenen Verzeichnis nach Geräten. Die Mitglieder werden unabhängig davon, ob der Computer an- oder ausgeschaltet ist, gefunden.
- **IPMI:** Sucht nach Servern mit aktiviertem Intelligent Platform Management Interface. Damit können Sie auf zahlreiche Funktionen zugreifen, unabhängig davon, ob der Server eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet.
- **Virtuelle Hosts:** Sucht nach Servern, auf denen VMware ESX Server ausgeführt wird. Diese Servers erscheinen im Ordner **Virtuelle Hosts**.

Um die Suche nach nicht verwalteten Geräten zu automatisieren, können Sie regelmäßige UDD-Scans planen. Sie können beispielsweise Ihr Netzwerk in Drittel unterteilen und zeitplangesteuert für jedes Drittel eine Ping-Suche pro Nacht durchführen.

Bei einer zeitplangesteuerten Erkennung übernimmt der Coreserver die Suche. Nicht nach Zeitplan organisierte Erkennungen werden von der Konsole ausgeführt, die diese startet.

Erweiterte Geräteerkennung

Das UDD-Tool unterstützt auch das Scannen der erweiterten Geräteerkennung (XDD). XDD verwendet dazu einen Geräteagenten (über eine Agentenkonfiguration bereitgestellt), die Ihr LANDesk-Netzwerk nach ARP- und WAP-Broadcasts abhört. Der XDD-Agent auf einem konfigurierten Gerät prüft dann nach, ob auf dem Broadcasting-Gerät der Standard LANDesk Agent installiert ist. Wenn der Standard LANDesk Agent nicht reagiert, wird in der Gruppe **Computer** ein ARP-erkanntes Gerät mit seinem Bericht in der Listenansicht dargestellt und in der Gruppe **Wireless Access Points** ein WAP-Gerät mit seinem Bericht.

Die erweiterte Geräteerkennung leistet optimale Dienste in Situationen, in denen Firewalls Geräte daran hindern, auf die normalen pinggestützte UDD-Erkennungsmethoden zu antworten.

HINWEIS: Verwenden Sie die "Erweiterte Geräteerkennung" zum Ermitteln von Firewall-Geräten
Denken Sie daran, dass die regulären Methoden für die "Erkennung nicht verwalteter Geräte" normalerweise keine Geräte erkennen können, die eine Firewall verwenden, z. B. die in Windows integrierte Windows Firewall. Die Firewall hindert das Gerät normalerweise daran, auf die Erkennungsmethoden zu reagieren, die von der "Erkennung nicht verwalteter Geräte" verwendet wird.. Die erweiterte Geräteerkennung löst dieses Problem, indem Sie über den ARP-Datenverkehr im Netz Geräte erkennt.

Verwandte Themen

"Bereitstellen von LANDesk-Agenten auf nicht verwalteten Geräten" auf Seite 363

"Erkennen nicht verwalteter Geräte mit UDD" auf Seite 364

"Mit Geräten arbeiten, die über XDD gefunden wurden" auf Seite 372

"Was geschieht, wenn ein Gerät erkannt wird?" auf Seite 370

"Verwendung der erweiterten Geräteerkennung (mit ARP und WAP)" auf Seite 367

"Hilfe zur "Erkennung nicht verwalteter Geräte"" auf Seite 373

Bereitstellen von LANDesk-Agenten auf nicht verwalteten Geräten

Nachdem Sie nicht verwaltete Geräte mit den o.g. Scan- und Erkennungsmethoden erkannt haben, können Sie anhand der folgenden Methoden auf diesen Geräten LANDesk Agenten bereitstellen.

- Über pushbasierte Bereitstellungen mithilfe von geplanten Aufgaben und einem Domänenverwaltungskonto, das Sie für den Scheduler konfiguriert haben.
- Über pushbasierte Bereitstellungen mithilfe des Standard LANDesk Agent. Wenn auf den Geräten der Standard LANDesk Agent installiert ist, können Sie eine pushbasierte Bereitstellung durchführen.
- Über eine pullbasierte Bereitstellung mithilfe eines Anmeldeskripts.

Weitere Information zur Bereitstellung von Geräten finden Sie bei der LANDesk Benutzercommunity unter http://community.landesk.com.

Wenn Sie Geräte für die agentenbasierte Bereitstellung ordnen, ist es u. U. einfacher, die Liste der nicht verwalteten Geräte nach Standard LANDesk Agent (für Standard LANDesk Agent-Gerätebereitstellungen) und nach Domäne (für Bereitstellungen mithilfe von geplanten Tasks) zu sortieren.

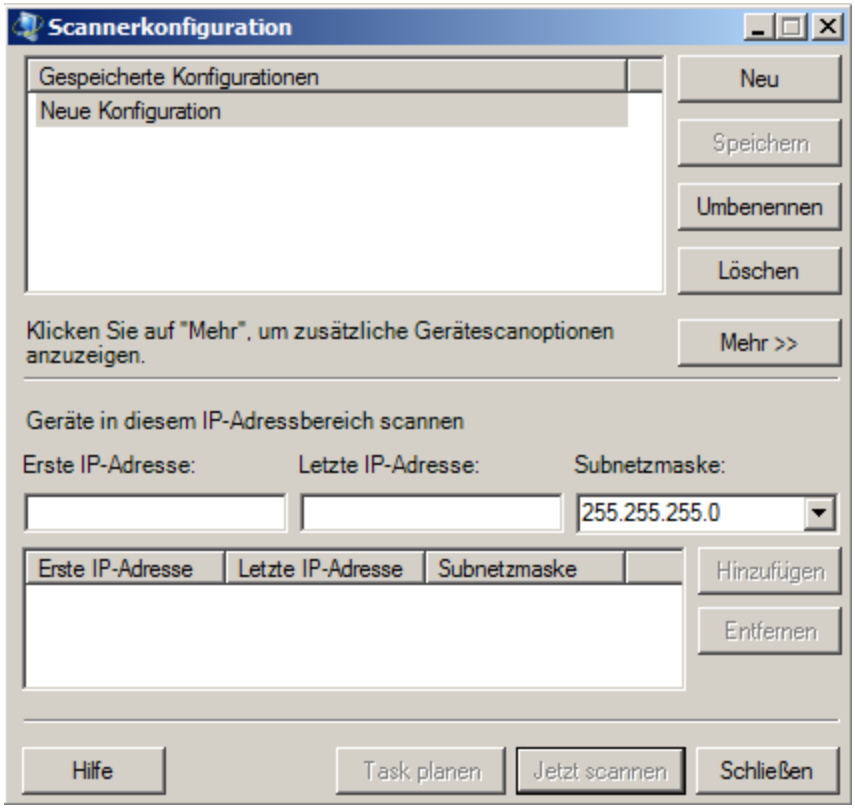
HINWEIS: Bereitstellung auf Windows XP-Geräten
Die Windows-Standardeinstellung erzwingt Netzwerkanmeldungen, die ein lokales Konto zur Anmeldung verwenden, stattdessen das Gästekonto zu verwenden. Wenn Sie ein Administratorkonto auf Domänenebene und ein lokales Konto für den Scheduler-Dienst verwenden, misslingen geplante Tasks, weil der Scheduler-Dienst die Authentifizierung nicht durchführen kann.

So stellen Sie LANDesk Agenten auf nicht verwalteten Geräten bereit

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration** und erstellen Sie eine neue Konfiguration oder verwenden Sie eine vorhandene Konfiguration. Klicken Sie im Kontextmenü der Konfiguration auf **Planen**.
2. Klicken Sie auf **Extras > Konfiguration > Erkennung nicht verwalteter Geräte** und wählen Sie die Geräte aus, auf denen Sie Agenten bereitstellen möchten. Ziehen Sie die Geräte in das Fenster **Geplante Tasks**. Wenn das Fenster **Geplante Tasks** eine minimierte Registerkarte ist, können Sie Geräte auf die Registerkarte **Geplante Tasks** ziehen. Hierbei wird das Fenster **Geplante Tasks** geöffnet.
3. Wenn auf den Geräten der Standard LANDesk Agent installiert ist, klicken Sie auf **Konfigurieren > Dienste** und dann auf die Registerkarte **Scheduler**. Stellen Sie sicher, dass das Scheduler-Konto auf den Geräten, auf denen Sie Agenten bereitstellen möchten, über Administratorrechte verfügt.
4. Doppelklicken Sie auf das Bereitstellungsskript und legen Sie eine Startzeit fest. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben.
5. Überprüfen Sie das Fenster **Geplante Tasks** auf Aktualisierungen.

Erkennen nicht verwalteter Geräte mit UDD

Mit den grundlegenden UDD-Scanmethoden können Sie nicht verwaltete Geräte ganz einfach erkennen.



So erkennen Sie nicht verwaltete Geräte mit UDD

1. Klicken Sie im Fenster "Erkennung nicht verwalteter Geräte" (**Extras > Konfiguration > Erkennung nicht verwalteter Geräte**) auf die Schaltfläche **Netzwerk scannen**.
2. Klicken Sie auf **Mehr >>** und wählen Sie die gewünschten Erkennungsoptionen aus. Bei Standard-Erkennungstyp kommt ein Standard-Netzwerkscan mit IP-Betriebssystem-Fingerabdruck für die erkannten Geräte zum Einsatz.
3. Geben Sie einen Anfangs- und End-IP-Bereich für den Scan ein. Sie müssen einen Bereich eingeben, damit die **Standard LANDesk Agentenerkennung** (CBA) oder die **Netzwerkerkennung** ausgeführt werden kann. Der Bereich ist optional für die **NT-Domäne** und für **LDAP**.
4. Geben Sie eine **Subnetzmaske** ein.
5. Klicken Sie auf die Schaltfläche **Hinzufügen**, um den soeben konfigurierten Scan zur Taskliste hinzuzufügen.
6. Wählen Sie in der Taskliste unten im Dialogfeld die Scans aus, die Sie ausführen möchten, und klicken Sie auf die Schaltfläche **Jetzt scannen** (um den Scan sofort auszuführen) bzw. auf die Schaltfläche **Task planen** (um die Scans später oder auf der Basis eines sich wiederholenden Zeitplans auszuführen). Die Schaltflächen **Jetzt scannen** und **Task planen** führen nur Scans aus, die Sie zur Taskliste hinzugefügt haben und die ausgewählt sind.
7. Aktualisierungen des Scanstatus werden im Fenster "Scanstatus" angezeigt. Wenn der Scan beendet ist, klicken Sie in den Dialogfeldern "Scanstatus" und "Scannerkonfiguration" auf **Schließen**.
8. Klicken Sie in der UDD-Strukturansicht auf **Computer**, um die Scanergebnisse anzuzeigen.

Konfigurieren der Windows NT-Domänenerkennung

Die Windows NT-Domänenerkennung ist nur funktionsfähig, wenn Sie den Scheduler-Dienst so konfigurieren, dass er sich bei der Domäne mit einem Domänenadministratorkonto anmeldet.

So konfigurieren Sie das Scheduler-Anmeldekonto

1. Klicken Sie auf **Konfigurieren > Dienste** und anschließend auf die Registerkarte **Scheduler**.
2. Klicken Sie auf **Anmeldung ändern**.
3. Geben Sie den Benutzernamen und das Kennwort eines Domänenadministrators ein.
4. Klicken Sie auf **OK**.
5. Starten Sie den Scheduler-Dienst neu, damit die Änderungen übernommen werden. Klicken Sie auf der Registerkarte **Scheduler** auf **Stopp** und auf **Start**, nachdem der Dienst gestoppt wurde.

Verwaltung der Berichte zu ARP-erkannten Geräten

UDD speichert Geräte, die über die erweiterte Geräteerkennung ermittelt wurden, in der Datenbank des Coreservers. Wenn Sie über eine große Anzahl nicht verwalteter Geräte verfügen, kann diese Datenmenge äußerst schnell an Volumen zunehmen. Standardmäßig werden diese Daten 24 Stunden aufbewahrt. Sie können festlegen, wie viel Zeit vergehen darf, bis Geräte, die über die erweiterte Geräteerkennung gefunden wurden, aus der Datenbank entfernt werden. Nach der von Ihnen angegebenen Anzahl von Tagen werden Geräte, die innerhalb dieses Zeitraums nicht neu wieder erkannt wurden, gelöscht.

So konfigurieren Sie den ARP-Erkennungsverlauf

1. Klicken Sie auf **Tools > Konfiguration > Erkennung nicht verwalteter Geräte**.
2. Klicken Sie auf die Symbolleistenschaltfläche **ARP-Erkennungsverlauf konfigurieren**.
3. Ändern Sie die gewünschten Optionen. Klicken Sie auf **Hilfe**, um weitere Informationen zu erhalten.
4. Klicken Sie abschließend auf **OK**.

Wiederherstellen von Clientdatensätzen

Sollten Sie jemals Ihre Coredatenbank zurücksetzen und gezwungen sein, Gerätedaten wiederherzustellen, können Sie mithilfe von UDD alle Geräte im Netzwerk erkennen lassen. Anschließend können Sie die Ergebnisse des Erkennungsvorgangs als Ziel für den geplanten Task "Clientdatensätze wiederherstellen" verwenden.

Wenn der Standard LANDesk Agent auf den Geräten installiert ist, veranlasst dieser Task, dass die Geräte einen vollständigen Inventarscan an die Coredatenbank senden, für die jedes Gerät lokal konfiguriert ist. Als Ergebnis dieses Tasks werden diejenigen Geräte, die bereits konfiguriert sind, zurück in die Datenbank gescannt. Die Geräte zeigen dann immer noch auf den richtigen sie verwaltenden Coreserver. Der Task misslingt auf Geräten, die nicht von einem Coreserver verwaltet werden.

So stellen Sie Clientdatensätze wieder her

1. Verwenden Sie UDD - wie bereits beschrieben - zur Erkennung nicht verwalteter Geräte.
2. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
3. Klicken Sie im Fenster **Geplante Tasks** auf die Schaltfläche **Geplantes**.
4. Klicken Sie auf **Clientdatensätze wiederherstellen** und vom Kontextmenü aus auf **Planen**.

5. Ziehen Sie die Computer, die Sie wiederherstellen möchten, aus der UDD-Strukturansicht **Ergebnisse suchen** auf den Task **Clientdatensätze wiederherstellen** im Fenster **Geplante Tasks**.
6. Klicken Sie im Kontextmenü des Tasks **Clientdatensätze wiederherstellen** auf **Eigenschaften** und konfigurieren Sie den Task.
7. Überprüfen Sie das Fenster **Geplante Tasks** auf Aktualisierungen.

Grundlegendes zur IP-Adressenfilterung mit erweiterter Geräteerkennung (XDD)

Es wird davon abgeraten, die erweiterte Geräteerkennung (XDD, eXtended Device Discovery) auf Notebook-Computern zu installieren, da diese Computer möglicherweise Verbindungen mit anderen Netzwerken herstellen, die Sie nicht überwachen möchten, z. B. Hotel- und Flughafennetzwerke. Um die Erkennung von Geräten zu verhindern, die nicht Bestandteil Ihres Netzwerkes sind, ignorierter der Coreserver IP-Adressen, bei denen das erste und zweite IP-Adress-Oktett plus 10 oder minus 10 von dem des Coreserver-Oktetts beträgt. Wenn die IP-Adresse Ihres Coreservers beispielsweise 192.168.20.17 lautet, ignoriert die erweiterte Geräteerkennung auf dem Coreserver Adressen über 203.179.0.0 und unter 181.157.0.0.

Sie können diese Funktion deaktivieren, indem Sie den folgenden DWORD-Registrierungsschlüssel dem Coreserver hinzufügen und seinen Wert auf 0 setzen:

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\Filter

Sie können den Filterwert auf 1 setzen, um die Filterung wieder zu aktivieren.

Sie können die ersten und zweiten Oktett-Überwachungsbereiche anpassen, indem Sie die folgenden DWORD-Registrierungsschlüssel dem Coreserver hinzufügen und ihre Werte auf den numerischen Bereich setzen, den Sie überwachen möchten (der Standard ist 10 für die ersten und zweiten Oktette):

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold1
- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\XDD\FilterThreshold2

FilterThreshold1 enthält den Bereich des ersten Oktetts und FilterThreshold2 den für das zweite Oktett.

Verwendung der erweiterten Geräteerkennung (mit ARP und WAP)

Die erweiterte Geräteerkennung (XDD) arbeitet außerhalb der normalen scanbasierten Erkennungsmethoden, die von UDD eingesetzt werden. Der XDD-Agent kann konfiguriert und auf verwalteten Geräten bereitgestellt werden, um ARP und/oder WAP-Erkennungsmethoden zu verwenden. In diesem Abschnitt werden beide Erkennungsmethoden beschrieben.

ARP Erkennungsmethode

Verwaltete Geräte, die mit dem XDD-Erkennungsagenten für ARP-Erkennung konfiguriert sind, suchen nach ARP-Broadcasts (Address Resolution Protocol) und erhalten ein Cache (sowohl im Speicher als auch in einer Datei auf dem lokalen Laufwerk) der Geräte, die sie herstellen. Vernetzte Geräte verwenden ARP, um eine TCP/IP-Adresse mit der MAC-Adresse der Netzwerkhardware eines spezifischen Geräts zu verknüpfen. Diese Kommunikation findet auf einem sehr niedrigen Level statt und verlässt sich nicht auf Geräte, die auf Pings oder Agentenkommunikationsdaten an bestimmten Netzwerkanschlüssen reagieren. Selbst stark Firewall-geschützte Geräte verlassen sich auf ARP. Aus diesem Grund kann die erweiterte Geräteerkennung Ihnen helfen, Geräte ausfindig zu machen, die von normalen Erkennungsscans nicht erfasst werden.

Wenn ein neuer ARP-Broadcast von einem Gerät erkannt wird, das mit dem erweiterten Geräteerkennungsagenten konfiguriert wurde, warten die Agenten, die das ARP wahrgenommen haben, zwei Minuten lang auf den Bootvorgang des erkannten Geräts, und dann wartet jeder Agent eine willkürliche Zeitspanne. Der Agent mit der kürzesten willkürlichen Wartezeit führt zuerst einen Zeit-Pingtest mit den neuen Gerät durch (zur Ermittlung von LANDesk-Agenten); anschließend sendet UDP einen Broadcast an das Subnetz, um die anderen Agenten wissen zu lassen, dass es den Pingtest für dieses Gerät bereits ausgeführt hat. Wenn Sie mehrere Agenten der erweiterten Geräteerkennung installiert haben, verhindern Sie hiermit, dass Geräte im überhöhtem Maße Netzwerkdaten generieren, da alle gleichzeitig dem Pingtest unterzogen werden.

Die vom Agenten der erweiterten Geräteerkennung gespeicherten ARP-Tabellen werden nach 48 Stunden standardmäßig durch ein Timeout beendet. Dies bedeutet, dass jedes Netzwerkgerät ein Mal pro Timeout-Zeitspanne einem Ping-Test unterzogen wird. Selbst mit Geräten, die große Mengen ARP-Daten erzeugen, wird nur ein Mal pro Timeout-Zeitspanne ein Pingtest durchgeführt.

Geräte, auf denen LANDesk-Agenten installiert sind, gelten als verwaltet und werden nicht dem Coreserver gemeldet. Geräte ohne LANDesk-Agenten werden dem Coreserver als nicht verwaltete Geräte gemeldet. Diese Geräte werden in der Liste **Computer** des Fensters **Erkennung nicht verwalteter Geräte** angezeigt. Für ARP-erkannte Geräte wird in der Spalte **ARP Erkannt** der Wert **Wahr** angezeigt. Für nicht verwaltete Geräte, die mit ARP erkannt wurden, berichtet XDD folgende Informationen in den Spalten der Listenansicht:

- IP-Adresse
- MAC-Adresse
- Zuerst gescannt
- Zuletzt gescannt
- Male gescannt

WAP Erkennungsmethode

Sie können verwaltete Geräte auch so konfigurieren, dass sie Geräte mit WAP (Wireless Access Point) in Ihrem Netzwerk wahrnehmen und jedes erkannte WAP-Gerät der Gruppe Wireless Access Points dem Tool "Erkennung nicht verwalteter Geräte" hinzufügen.

Für Geräte, die mit WAP erkannt wurden, berichtet XDD folgende Informationen in den Spalten der Listenansicht:

- Gerätename
- MAC-Adresse
- Zuerst gescannt
- Zuletzt gescannt
- Male gescannt
- WAP-Zustand (zulässig, Rogue, aktive Ausnahme)
- Signalstärke (zur Feststellung des ungefähren Standorts des WAP-Geräts)
- Verschlüsselungsgrad (das vom WAP-Gerät verwendete Verschlüsselungsschema)
- Hersteller

HINWEIS: Berichten der MAC-Adresse
XDD verwendet die API Wireless-Erkennung auf Geräten mit Windows Vista und Windows 7, um die MAC-

Adresse des Geräts zu erhalten und in der Listenansicht anzuzeigen. Diese Funktion wird jedoch nicht auf Geräten mit Windows XP unterstützt.

Konfiguration der Geräte zur Verwendung der erweiterten Geräteerkennung (ARP und WAP)

Sie können einige ihrer verwalteten Geräte mit dem Agentenkonfigurationstool mit dem erweiterten Geräteerkennungsagenten (XDD) konfigurieren, damit sie als Erkennungsgeräte fungieren können, die das Netzwerk nach ARP- und WAP-Signalen abhören.

Sie müssen die erweiterte Geräteerkennung nicht auf jedem verwalteten Gerät bereitstellen. Die Bereitstellung des XDD-Agenten auf mehreren Geräten in jedem Ihrer Subnetze sollte ausreichend sein.

So stellen Sie den erweiterten Geräteerkennungsagenten für die ARP- und/oder WAP-Erkennung bereit

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neu**.
3. Geben Sie einen **Konfigurationsnamen** ein.
4. Wählen Sie im Dialogfeld **Agentenkonfiguration** auf der Seite **Erweiterte Geräteerkennung** eine oder beide Erkennungsmethoden aus, die Sie bereitstellen möchten.
5. Geben Sie eine Einstellung für die von Ihnen ausgewählten Erkennungsmethoden an. Sie können eine bestehende Einstellung aus der Liste auswählen oder auf **Konfigurieren** klicken, um eine Einstellung zu bearbeiten oder eine neue Einstellung für diese Agentenkonfiguration zu erstellen.
6. Schließen Sie die Angabe der Optionen in der Agentenkonfiguration ab. Für weitere Informationen zu einer beliebigen Seite klicken Sie auf **Hilfe**.
7. Klicken Sie auf **Speichern**.
8. Stellen Sie die Agentenkonfiguration auf den gewünschten Zielgeräten in jedem einzelnen Subnetz bereit.

Sie können mehrere unterschiedliche Einstellungen der erweiterten Geräteerkennung für Geräte konfigurieren, auf denen der Agent für die erweiterte Geräteerkennung installiert ist. Dieser Agent synchronisiert seine Einstellungen in regelmäßigen Abständen mit dem Coreserver.

So konfigurieren Sie die Einstellungen des erweiterten Geräteerkennungsagenten für die ARP- und/oder WAP-Erkennung

1. Klicken Sie auf **Tools > Konfiguration > Erkennung nicht verwalteter Geräte**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Erweiterte Geräteerkennung konfigurieren** und wählen Sie aus, welchen Einstellungstyp Sie für die Erkennungsmethode konfigurieren möchten (ARP oder WAP).
3. Geben Sie die Scanoptionen für die Erkennungsmethode an. Für detaillierte Informationen klicken Sie auf **Hilfe**.
4. Klicken Sie abschließend auf **OK**. Bei der nächsten Synchronisierung der erweiterten Geräteerkennung mit dem Coreserver, werden Ihre Änderungen übernommen.

Verwendung der Berichte der erweiterten Geräteerkennung

Im Fenster **Berichte** (**Extras > Berichte / Überwachung** auf **Berichte > Nicht verwaltete Geräte** klicken) werden mehrere XDD-Berichte angezeigt, die Sie einsehen können.

Berichte der erweiterten Geräteerkennung umfassen:

- **ARP-Geräteerkennungsverlauf:** Verlaufsdaten zu nicht autorisierten Geräten.
- **Aktuelles ARP hat Geräte ohne den Agenten erkannt:** Geräte, auf den der LANDesk Agent derzeit entweder deaktiviert oder nicht funktionsfähig ist.
- **Verlauf der ARP-Geräteerkennung ohne den Agenten:** Verlaufsdaten zu Geräten, auf den der LANDesk Agent entweder deaktiviert oder nicht funktionsfähig ist.
- **Nicht verwaltete Geräte:** Zeigt alle Geräte im Netzwerk an, die keinem Coreserver zugeordnet sind.
- **Wirelessgeräte:** Verlauf aller Wirelessgeräte, die erkannt wurden.

Was geschieht, wenn ein Gerät erkannt wird?

Wenn UDD oder XDD ein nicht verwaltetes Gerät zum ersten Mal finden, versuchen sie, den Gerätetyp zu identifizieren, um ihn einer der folgenden Gruppen zuzuordnen:

- **Computer:** Enthält durch UDD-Scanmethoden (und die ARP-Erkennungsmethode des XDD-Agenten) erkannte Geräte.
- **Suchergebnisse:** Enthält Suchergebnisse.
- **Infrastruktur:** Umfasst Router und andere Netzwerk-Hardware.
- **Intel vPro:** Enthält Intel vPro-aktivierte Geräte.
- **IPMI:** Enthält Server, die über das Intelligent Platform Management Interface verfügen.
- **Andere:** Enthält nicht identifizierte Geräte.
- **Drucker:** Enthält Drucker.
- **Virtuelle Hosts:** Enthält virtuelle Hosts.
- **Wireless Access Points:** Führt erkannte (vom XDD-Agenten ermittelte) WAP-Geräte auf.

Dank dieser Gruppen bleibt die UDD-Liste übersichtlich. Auf diese Weise lassen sich die Geräte, für die Sie sich interessieren, leichter finden. Sie können die Geräteliste nach einer Spaltenüberschrift sortieren, indem Sie auf die gewünschte Spaltenüberschrift klicken.

HINWEIS: Geräte in andere Gruppen verschieben
UDD ordnet die Geräte möglicherweise nicht in die richtigen Kategorien ein und legt sie daher nicht immer in den entsprechenden Gerätegruppen ab. Wenn dies vorkommt, können Sie falsch identifizierte Geräte einfach in die korrekte Gruppe ziehen.

UDD versucht, grundlegende Informationen über das Gerät zu erkennen und zu berichten, einschließlich der folgenden Daten, die in der Elementelistenansicht im rechten Fensterabschnitt des Extras-Fensters erscheinen:

- **Gerätename:** Der Name des erkannten Geräts, falls verfügbar.
- **IP-Adresse:** Die ermittelte IP-Adresse. Sie wird von UDD immer angezeigt. Von XDD nicht.
- **Subnetzmaske:** Die erkannte Subnetzmaske. Sie wird von UDD immer angezeigt.
- **Betriebssystembeschreibung:** Die ermittelte Betriebssystembeschreibung, falls verfügbar.

- **MAC-Adresse:** Die erkannte MAC-Adresse; diese wird üblicherweise zurückgegeben, wenn das Gerät über den Standard LANDesk Agenten oder NetBIOS verfügt bzw. wenn sich das Gerät im selben Subnetz wie der Coreserver oder die Konsole befindet, der/die die Suche durchführt.
- **Gruppe:** Die UDD-Gruppe, der das Gerät angehört.
- **Standard LANDesk Agent:** Gibt an, ob das Gerät über CBA verfügt. Sie können andere LANDesk Agenten direkt auf den verwalteten Geräten bereitstellen, auf denen CBA geladen ist.
- **Alle Benutzer:** Am überprüften Gerät angemeldete Benutzer, falls vorhanden.
- **Gruppe/Domäne:** Die Gruppe/Domäne, der das Gerät angehört, falls vorhanden.
- **Zuerst gescannt:** Das Datum, an dem UDD das Gerät zum ersten Mal überprüft hat.
- **Zuletzt gescannt:** Das Datum, an dem UDD das Gerät zum letzten Mal überprüft hat. Mithilfe dieser Spalte finden Sie nicht verwaltete Geräte, die sich nicht mehr im Netzwerk befinden, oder die erst vor kurzem gefunden wurden.
- **Male gescannt:** Gibt an, wie oft UDD dieses Gerät überprüft hat.
- **ARP Erkannt:** Gibt an, ob das Gerät von ARP erkannt wurde.
- **XDD-Ausnahme:** Gibt an, ob das Gerät eine XDD-Ausnahme darstellt.
- **IPMI GUID:** Die IPMI GUID des Geräts, falls verfügbar.

Je nach Gerät kann UDD möglicherweise nicht für alle Spalten Daten liefern. Wenn UDD ein Gerät zum ersten Mal findet, sucht sie in der Coredatenbank nach der IP-Adresse und dem Namen des Geräts. Wenn diese Daten bereits in der Datenbank enthalten sind, ignoriert UDD das Gerät. Sind diese Daten noch nicht vorhanden, so fügt UDD das Gerät zur Tabelle der nicht verwalteten Geräte hinzu. In dieser Tabelle enthaltene Geräte verwenden keine LANDesk Lizenz. Ein Gerät gilt als verwaltet, sobald es einen Inventarscan an die Coredatenbank sendet. Sie können Geräte nicht aus UDD in die Netzwerkansicht der Hauptkonsole ziehen. Sobald nicht verwaltete Geräte einen Inventarscan gesendet haben, werden sie aus UDD entfernt und automatisch zur Netzwerkansicht hinzugefügt.

Sie können benutzerdefinierte Gruppen erstellen, um nicht verwaltete Geräte weiter einzustufen. Wenn Sie ein Gerät in eine andere Gruppe verschieben, lässt UDD es bei einer späteren Erkennung in dieser Gruppe. Neue Geräte in der Gruppe **Computer** sind leichter erkennbar, wenn Sie die Hauptgruppe **Computer** übersichtlich ordnen und Geräte, von denen Sie wissen, dass Sie sie nicht mit LANDesk verwalten werden, in Untergruppen oder andere Kategorien verschieben. Wenn Sie eine Gruppe löschen, die Geräte enthält, verschiebt UDD die Geräte in die Gruppe **Sonstige**.

Wenn Sie in einem Schritt alle Geräte aus mehreren Gruppen löschen möchten, klicken Sie auf die Symbolleistenschaltfläche **Elemente aus Gruppen entfernen** und wählen Sie die Gruppen aus, aus denen sämtliche Geräte entfernt werden sollen.

Mit dem Feld **Suchen** in der Symbolleiste finden Sie in kürzester Zeit alle Geräte, die den von Ihnen angegebenen Suchkriterien entsprechen. Sie können nach Daten in einer bestimmten Spalte oder in allen Spalten suchen. Die Suchergebnisse werden in der Kategorie **Suchergebnisse** angezeigt. Beispiel: Verwenden Sie "Suchen", um nicht verwaltete Computer, auf denen CBA installiert ist, zu einer Gruppe zusammenzufassen. Hierfür müssen Sie eine Suchanfrage definieren, die nach "J" im Feld "Standard LANDesk Agent" sucht.

Sie können auch einen Alarm erstellen, wenn UDD nicht verwaltete Geräte findet. Der Name des Alarms, den Sie in der Alarmierung (**Extras > Konfiguration > Alarmierung**, auf **Core-Alarmregelsatz** klicken) konfigurieren müssen, lautet **Erkennung nicht verwalteter Geräte - nicht verwaltetes Gerät gefunden**.

Mit Geräten arbeiten, die über XDD gefunden wurden

Nicht verwaltete Geräte, die mit der ARP-Erkennungsmethode der erweiterten Geräteerkennung gefunden wurden, werden in der Liste **Computer** des Fensters **Erkennung nicht verwalteter Geräte** angezeigt. WAP-Geräte, die mit der WAP-Erkennungsmethode der erweiterten Geräteerkennung gefunden wurden, werden in der Liste **Wireless Access Points** des Fensters **Erkennung nicht verwalteter Geräte** angezeigt.

Von dieser Liste aus können Sie normale UDD-Aktionen ausführen, z. B. das Verschieben in andere Gruppen. Klicken Sie mit der rechten Maustaste auf ein Gerät, um auf sein Kontextmenü zuzugreifen und die darin enthaltenen Optionen zu verwenden.

Sie können auch Ausnahmen der erweiterten Geräteerkennung importieren und exportieren. Eine Ausnahme ist ein Gerät im Netzwerk, das nicht verwaltbar oder das dem Administrator zwar bekannt ist, von dem die erweiterte Geräteerkennung jedoch keine Meldung machen soll.

Diese Ausnahmen liegen in einem CSV-Textdateiformat vor, das aus kommabegrenzten IP- und MAC-Adressen besteht, in dieser Reihenfolge, ein Paar pro Zeile. Der Export von Ausnahmen schließt alle in der Datenbank gespeicherten Ausnahmen ein. Der Import von Ausnahmen überschreibt alle in der Datenbank gespeicherten Ausnahmen mit den Ausnahmen, die Sie in die Importdatei einschließen.

Exportieren und Importieren von Ausnahmen der Geräteerkennung

So exportieren Sie alle Ausnahmen der erweiterten Geräteerkennung

1. Klicken Sie auf **Tools > Konfiguration > Erkennung nicht verwalteter Geräte**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Erweiterte Geräteerkennungsausnahmen in CSV-Datei exportieren**.
3. Wählen Sie einen Ordner aus und weisen Sie der Datei einen Namen zu.
4. Klicken Sie auf **Speichern**.

So importieren Sie alle Ausnahmen der erweiterten Geräteerkennung

1. Erstellen oder aktualisieren Sie eine kommabegrenzte CSV-Datei, die die gewünschten Ausnahmen enthält.
2. Klicken Sie auf **Tools > Konfiguration > Erkennung nicht verwalteter Geräte**.
3. Klicken Sie auf die Symbolleistenschaltfläche **Ausnahmen der erweiterten Geräteerkennung aus CSV-Datei importieren**.
4. Wählen Sie die CSV-Datei aus und klicken Sie auf **Öffnen**.

Fehlerbehebung bei falschen Ergebnissen für die Betriebssystemversion

In manchen Umgebungen gibt eine nmap-Zuordnung zu einer IP-Adresse, die nicht Gebrauch ist, eine Antwort auf bestimmten Ports zurück, die für nmap verwirrend sein kann. Welche Ports eine Antwort zurückgeben und welche nicht, variiert von einer Umgebung zur nächsten. Wenn nmap keine korrekten Ergebnisse zur Betriebssystemversion zurückgibt bzw. als generelle Empfehlung sollte nmap auf die Kundenumgebung abgestimmt werden.

So nehmen Sie die Feinabstimmung für nmap vor

1. Bestimmen Sie mehrere IP-Adressen in der Umgebung, die nicht verwendet werden.
2. Geben Sie an einer Befehlszeilenaufforderung auf dem Coreserver folgende Befehlszeile ein, um die IP-Adressen manuell zu scannen:

   nmap -O -sSU -F -T4 -d -v <Ziele> -oX test.xml > test.txt

3. Prüfen Sie die Ergebnisse und kontrollieren Sie, ob es irgendwelche Ports gibt, die konsistent auf IP-Adressen reagieren, die nicht verwendet werden.
4. Öffnen Sie das nmap-services-Dokument von Management Suite (C:\Programme\LANDesk\Management Suite\nmap\nmap-services) und kommentieren Sie die Ports, die konsistent antworten, mit einem Rautenzeichen (#) aus.

Hilfe zur "Erkennung nicht verwalteter Geräte"

Auf das LANDesk Extra zur Erkennung nicht verwalteter Geräte (UDD) greifen Sie von der LANDesk-Hauptkonsole aus zu (**Extras > Konfiguration > Erkennung nicht verwalteter Geräte**). Mithilfe dieses Tools können Sie Geräte in Ihrem Netzwerk finden, die keinem Inventarscan der LANDesk Coredatenbank unterzogen wurden. UDD verwendet bei der Suche nach nicht verwalteten Geräten mehrere Methoden. Es unterstützt darüber hinaus die erweiterte Geräteerkennung (XDD), die mit einem Geräteagenten arbeitet, der das Netzwerk auf neue ARP- und WAP-Broadcasts abhört. Anschließend überprüft der Agent der erweiterten Geräteerkennung dann erkannte Geräte auf das Vorhandensein des LANDesk Agenten. Wenn der LANDesk Agent nicht reagiert, zeigt die erweiterte Geräteerkennung das Gerät in der Liste **Computer** an. Die erweiterte Geräteerkennung leistet optimale Dienste in Situationen, in denen Firewalls Geräte daran hindern, auf die normalen pinggestützte UDD-Erkennungsmethoden zu antworten.

Dieses Kapitel enthält die nachstehend aufgeführten Online-Hilfethemen, in denen die Dialogfelder des Extras "Erkennung nicht verwalteter Geräte" beschrieben werden. Von der Konsolenoberfläche aus können Sie diese Themen aufrufen, indem Sie auf die Schaltfläche **Hilfe** des jeweiligen Dialogfelds klicken.

Informationen zum Dialogfeld "Scannerkonfiguration"

Mit diesem Dialogfeld können Sie nicht verwaltete Gerätescans anpassen und starten. Um darauf zuzugreifen, klicken Sie im Extras-Fenster **Erkennung nicht verwalteter Geräte** auf die Schaltfläche **Netzwerk scannen** in der Symbolleiste.

- **Gespeicherte Konfigurationen:** Die gespeicherten Scannerkonfigurationen werden angezeigt. Sie speichern eine Konfiguration, indem Sie die Einstellungen Ihren Vorstellungen entsprechend ändern, auf **Neu** klicken, der Konfiguration einen Namen zuweisen, sie auswählen und anschließend auf **Speichern** klicken.
- **Mehr >>:** Erweitert das Dialogfeld, so dass die Erkennungsoptionen angezeigt werden.
- **Netzwerkscan:** Erkennt Geräte mithilfe einer ICMP-Ping-Suche. Diese Suchmethode ist die genaueste und daher empfohlene Erkennungsmethode.
  - **IP-Betriebssystem-Fingerabdruck:** Eine zusätzliche Ebene der Erkennung, bei der versucht wird, das auf einem erkannten Gerät installierte Betriebssystem anhand von Paketantworten zu bestimmen.
  - **SNMP verwenden:** Eine zusätzliche Erkennungsebene, bei der SNMP zur Geräteerkennung verwendet wird.

- **Geräte mit installiertem LANDesk CBA erkennen:** Erkennt Geräte, auf denen der CBA-Agent ausgeführt wird. Wenn Ihre Geräte über CBA verfügen, ist dies die schnellste Suchmethode.
    - **Geräte mit installiertem LANDesk PDS2 erkennen:** Erkennt Geräte, die den älteren LANDesk PDS2-Agenten verwenden. Sie können diese Option nur auswählen, wenn Sie zuvor **CBA-Erkennung** ausgewählt haben.
- **Geräte mithilfe von NT-Domäne erkennen:** Erkennt Geräte in einer Windows NT-Domäne. Diese Option verwendet die NT-Domänen-Kontodaten und benötigt keinen IP-Adressbereich; Sie können jedoch einen solchen angeben. Wählen Sie diese Option aus und klicken Sie auf **Konfigurieren**, um das Dialogfeld **NT-Domänenkonfiguration** anzuzeigen. Hier können Sie die Einstellungen für die NT-Domänenerkennung anpassen.
- **Nach IP-Bereich filtern** (für NT-Domäne und LDAP): Filtert die NT-Domäne und LDAP-Erkennung anhand der IP-Bereiche, die Sie unter **Erste IP-Adresse** und **Letzte IP-Adresse** angegeben haben.
- **Geräte mithilfe von LDAP erkennen:** Erkennt Geräte in einem LDAP-Verzeichnis. Wählen Sie diese Option aus und klicken Sie auf **Konfigurieren**, um das Dialogfeld **LDAP-Konfiguration** anzuzeigen. Hier können Sie die Einstellungen für die LDAP-Erkennung nach Bedarf anpassen.
- **IPMI-fähige Geräte erkennen:** Sucht nach Servern mit aktiviertem "Intelligent Platform Management Interface". Damit können Sie auf zahlreiche Funktionen zugreifen, unabhängig davon, ob der Server eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet.
- **Virtuelle Hosts erkennen:** Sucht nach Servern, auf denen VMware ESX Server ausgeführt wird.
- **Erste IP-Adresse:** Geben Sie die Start-IP-Adresse für den Adressbereich ein, den Sie scannen möchten.
- **Letzte IP-Adresse:** Geben Sie die Abschluss-IP-Adresse für den Adressbereich ein, den Sie scannen möchten. UDD aktualisiert dieses Feld automatisch, während Sie die **Start-IP-Adresse** eingeben; Sie können die Abschluss-IP-Adresse aber auch manuell ändern. Der Wert für die **Letzte IP-Adresse** wird aus dem Wert im Feld **Subnetzmaske** und dem Wert im Feld **Erste IP-Adresse** errechnet.
- **Subnetzmaske:** Geben Sie die Subnetzmaske für den IP-Adressbereich ein, den Sie überprüfen.
- **Hinzufügen** und **Entfernen:** Fügt die IP-Adressbereiche zur Warteschlange im unteren Abschnitt des Dialogfelds hinzu oder entfernt sie.
- **Task planen:** Der Scan wird anhand Ihrer Einstellungen geplant. Sie können die Startzeit im Fenster **Geplante Tasks** anpassen. Geplante Scans gehen vom Coreserver aus.
- **Jetzt scannen:** Startet den Scan sofort anhand Ihrer Einstellungen. Hier gestartete Scans gehen von der aktuellen Konsole aus. Sobald Sie den Scan gestartet haben, wird das Dialogfeld **Scanstatus** angezeigt. Sie können darin nachprüfen, wie viele Geräte gefunden, wie viele aktualisiert und wie viele neue, nicht verwaltete Geräte hinzugefügt wurden.

Informationen zum Dialogfeld "NT-Domänenkonfiguration"

In diesem Dialogfeld konfigurieren Sie die Verbindung zu der Domäne, die Sie überprüfen möchten.

- **Domäne:** Geben Sie die Domäne ein, die Sie überprüfen möchten.
- **Als aktueller Benutzer anmelden:** Wählen Sie diese Möglichkeit, wenn Sie als Benutzer mit Zugriff auf die Domäne, die Sie überprüfen, angemeldet sind.
- **Anmelden als:** Wählen Sie diese Möglichkeit, wenn Sie nicht als Benutzer mit Zugriff auf die Domäne, die Sie überprüfen, angemeldet sind. Geben Sie außerdem einen **Benutzernamen** und ein **Kennwort** ein.
- **Domäneninformationen verwenden:** Verwendet Informationen von der Domäne zum Betriebssystem des erkannten Geräts.

- **Hinzufügen** und **Entfernen:** Fügen Sie jede Domäne, die Sie konfigurieren und überprüfen möchten, zur Arbeitsschlange hinzu, indem Sie auf **Hinzufügen** klicken. Klicken Sie auf **Entfernen**, um die ausgewählte Domäne aus der Arbeitsschlange zu entfernen.

Informationen über das Dialogfeld "LDAP-Konfiguration"

In diesem Dialogfeld konfigurieren Sie die Verbindung zu dem LDAP-Verzeichnis, das Sie überprüfen möchten.

- **LDAP://:** Geben Sie das LDAP-Verzeichnis ein, das Sie überprüfen möchten.
- **Als aktueller Benutzer anmelden:** Wählen Sie diese Möglichkeit, wenn Sie als Benutzer mit Zugriff auf das Verzeichnis, das Sie überprüfen, angemeldet sind.
- **Anmelden als:** Wählen Sie diese Möglichkeit, wenn Sie nicht als Benutzer mit Zugriff auf das Verzeichnis, das Sie überprüfen, angemeldet sind. Geben Sie außerdem einen **Benutzernamen** und ein **Kennwort** ein.
- **Einzelne OUs auswählen:** Wählen Sie die OUs aus, die Sie überprüfen möchten. Klicken Sie auf **Hinzufügen**, um sie zur Arbeitsschlange hinzuzufügen. Klicken Sie auf **Entfernen**, um die ausgewählte OU aus der Arbeitsschlange zu löschen.
- **Aktiver Verzeichnispfad:** Zeigt den aktiven Verzeichnispfad an, falls vorhanden.

Konfigurieren von SNMP-Scans

Netzwerkscan-Erkennungen können SNMP verwenden. Abhängig von der SNMP-Konfiguration Ihres Netzwerks müssen Sie u. U. zusätzliche SNMP-Informationen in die "Erkennung nicht verwalteter Geräte" (UDD, Unmanaged Devices Discovery) eingeben. Klicken Sie neben der **SNMP**-Option auf **Konfigurieren**, um das Dialogfeld **SNMP-Konfiguration** anzuzeigen, das folgende Optionen enthält:

- **Versuche:** Wie oft UDD versucht, die SNMP-Verbindung aufzubauen.
- **Auf Antwort warten (Sekunden):** Wie lange UDD auf eine SNMP-Antwort warten soll.
- **Port:** An welchen Port UDD die SNMP-Abfragen senden soll.
- **Community-Name:** Der von UDD zu verwendende SNMP-Community-Name.
- **SNMP V3 konfigurieren:** UDD unterstützt auch SNMP V3. Klicken Sie auf diese Schaltfläche, um SNMP V3-Optionen im Dialogfeld **SNMP V3-Konfiguration** zu konfigurieren.

Das Dialogfeld **SNMP V3-Konfiguration** enthält folgende Optionen:

- **Benutzername:** Der Benutzername, den UDD für die Authentifizierung gegenüber dem SNMP-Remote-Dienst verwenden sollte.
- **Kennwort:** Das Kennwort für den SNMP-Remote-Dienst.
- **Authentifizierungstyp:** Der von SNMP verwendete Authentifizierungstyp. Kann **MD5**, **SHA** oder **Keiner** sein.
- Privacy-**Typ:** Die vom SNMP-Dienst verwendete Verschlüsselungsmethode. Kann **DES**, **AES128** oder **Keiner** sein.
- Privacy-**Kennwort:** Das mit dem angegebenen Privacy-Typ zu verwendende Kennwort. Nicht verfügbar, wenn Sie für "Privacy-Typ" die Option **Keiner** ausgewählt haben.

Informationen zum Dialogfeld "ARP- (oder WAP-) Erkennungseinstellungen"

Mithilfe dieses Dialogfelds können Sie Ihre ARP- und WAP-Einstellungen verwalten, die zur erweiterten Geräteerkennung verwendet werden. Nachdem Sie die XDD-Einstellungen konfiguriert haben, können Sie sie zum Scannen von Tasks verwenden.

Dieses Dialogfeld enthält folgende Optionen:

- **Neu:** Öffnet das Dialogfeld "Einstellungen". In diesem Dialogfeld können Sie die Optionen der Erkennungsmethoden konfigurieren.
- **Bearbeiten:** Öffnet das Dialogfeld "Einstellungen". In diesem Dialogfeld können Sie die ausgewählten Einstellungen bearbeiten.
- **Kopieren:** Öffnet eine Kopie der ausgewählten Einstellung als Vorlage, die von Ihnen dann bearbeitet und umbenannt werden kann. Dies kann sich als nützlich erweisen, wenn Sie Einstellungen geringfügig ändern und für einen bestimmten Zweck speichern möchten.
- **Löschen:** Entfernt die ausgewählte Einstellung aus der Datenbank.
  Beachten Sie, dass die ausgewählte Einstellung möglicherweise mit Tasks oder verwalteten Geräten verknüpft ist. Wenn Sie diese Einstellung löschen, verfügen Geräte mit dieser Einstellung weiterhin über diese Einstellung und verwenden sie auch nach wie vor, bis ein neuer Agentenkonfigurationstask bereitgestellt wird. Geplante Tasks mit dieser Einstellung werden weiterhin auf Zielgeräten ausgeführt, genauso wie Local Scheduler-Tasks mit dieser Einstellung. Auch sie werden solange ausgeführt, bis eine neue Konfiguration bereitgestellt wird.
- **Schließen:** Schließt das Dialogfeld, ohne eine Einstellung auf den Task anzuwenden.

Informationen zum Dialogfeld "ARP-Erkennungseinstellungen konfigurieren"

Dieses Dialogfeld (Symbolleistenschaltfläche **Erweiterte Geräteerkennung konfigurieren** > **ARP-Erkennungseinstellungen konfigurieren**) verwenden Sie, um ARP-basierte Scaneinstellungen für die erweiterte Geräteerkennung zu konfigurieren.

- **Konfigurationsname:** Kennzeichnet die Einstellung mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Einstellungen" in einem Einstellungstask-Dialogfeld angezeigt.
- **Länge der Zwischenspeicherung der ARP-Eingabestatistiken (in Sekunden)** Gibt an, wie lange Geräte, die über den Agenten der erweiterten Geräteerkennung verfügen, eine Adresse in der ARP-Tabelle aufbewahren. Mit Geräten im ARP-Zwischenspeicher wird nach dem erstmaligen Erkennungsping kein weiterer Pingtest durchgeführt. Der Standardwert ist 24 Stunden (86.400 Sekunden). Der Mindestwert ist 900 Sekunden.
- **Maximale Verzögerung (in Sekunden), bevor für den LANDesk Agent ein Pingtest für ein unbekanntes Gerät ausgeführt wird:** Wenn ein neues ARP von einem Gerät erkannt wird, das über den Agenten der erweiterten Geräteerkennung verfügt, wartet das Gerät zwei Minuten auf den Bootvorgang des erkannten Geräts; anschließend wartet es dann einen willkürlichen Zeitraum innerhalb des von Ihnen hier angegebenen Wertes. Der Agent mit der kürzesten willkürlichen Wartezeit führt zuerst einen Pingtest durch; anschließend sendet UDP einen Broadcast an das Subnetz, um die anderen Agenten wissen zu lassen, dass es den Pingtest für dieses Gerät ausgeführt hat. Wenn Sie mehrere Agenten der erweiterten Geräteerkennung installiert haben, verhindern Sie hiermit, dass Geräte im überhöhtem Maße Netzwerkdaten generieren, da alle gleichzeitig dem Pingtest unterzogen werden. Wenn Sie diesen Wert zu hoch setzen, verlassen nicht verwaltete Geräte möglicherweise das Netzwerk, bevor mit ihnen ein Pingtest durchgeführt werden kann. Wenn Sie diesen Wert zu niedrig setzen, führen ggf. mehrere Agenten den Pingtest durch und melden dasselbe Gerät. Der Standardwert ist eine Stunde (3.600 Sekunden).

- **Aktualisierungshäufigkeit (in Sekunden) für die ARP-Tabelle:** Gibt an, wie oft das Gerät den ARP-Zwischenspeicher auf die Platte schreibt, um Datenverluste zu vermeiden, falls ein Gerät abgeschaltet wird, ausfällt oder neu bootet. Der Standardwert ist fünf Minuten (300 Sekunden).
- **Protokolliergrad:** Der Protokolliergrad für die lokale erweiterte Geräteerkennung für Fehler (1), Warnungen (2) oder Alles (3). Der Standard ist 1 - Nur Fehler. Protokolle werden in C:\Programme\LANDesk\LDClient\xddclient.log gespeichert.
- **Protokolliergrad erzwingen:** Überschreibt die Protokolliergrad-Einstellungen des Coreservers. Wenn Sie diese Option deaktivieren, können Sie den Protokolliergrad auf Geräten manuell festlegen. Dies kann nützlich sein für die Fehlerbehebung auf einem bestimmten Gerät, da Sie den Protokolliergrad dann nicht auf allen Geräten ändern müssen. Diese Funktion ist standardmäßig aktiviert.

Informationen zum Dialogfeld "WAP-Erkennungseinstellungen konfigurieren"

Dieses Dialogfeld (Symbolleistenschaltfläche **Erweiterte Geräteerkennung konfigurieren** > **WAP-Erkennungseinstellungen konfigurieren**) verwenden Sie, um WAP-basierte Scaneinstellungen für die erweiterte Geräteerkennung zu konfigurieren.

Dieses Dialogfeld enthält folgende Optionen:

- **Konfigurationsname:** Kennzeichnet die Einstellung mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Einstellungen" in einem Einstellungstask-Dialogfeld angezeigt.
- **Häufigkeit des WAP-Scans (in Sekunden):** Gibt an, wie oft der erweiterte Geräteerkennungsagent nach WAPs scannt.
- **Protokolliergrad:** Der Protokolliergrad für die lokale erweiterte Geräteerkennung für Fehler (1), Warnungen (2) oder Alles (3). Der Standard ist 1 - Nur Fehler. Protokolle werden in C:\Programme\LANDesk\LDClient\xddclient.log gespeichert.
- **Protokolliergrad erzwingen:** Überschreibt die Protokolliergrad-Einstellungen des Coreservers. Wenn Sie diese Option deaktivieren, können Sie den Protokolliergrad auf Geräten manuell festlegen. Dies kann nützlich sein für die Fehlerbehebung auf einem bestimmten Gerät, da Sie den Protokolliergrad dann nicht auf allen Geräten ändern müssen. Diese Funktion ist standardmäßig aktiviert.

Informationen zum Dialogfeld "ARP-Erkennungsverlauf"

Dieses Dialogfeld (Symbolleistenschaltfläche **ARP-Erkennungsverlauf konfigurieren**) verwenden Sie, um festzulegen, wie der Coreserver den ARP-Erkennungsverlauf handhabt. Diese Verlaufsdaten werden für die Erstellung von Berichten zur erweiterten Geräteerkennung verwendet. Die Optionen in diesem Dialogfeld wirken sich nicht auf die erkannten Geräte aus, die im Hauptfenster der Erkennung nicht verwalteter Geräte zu sehen sind. Dieser Verlauf gilt nur für Geräte, die mit der ARP-Erkennung erkannt wurden und auf denen keine LANDesk Agenten installiert sind.

- **Verlauf für diese Anzahl von Tagen führen:** Wenn Sie auf diese Option klicken, können Sie angeben, für wie viele Tage ARP-Verlaufsdaten in der Datenbank gespeichert werden sollen. ARP-Verlaufsdaten, die länger als die von Ihnen angegebene Anzahl von Tagen in der Datenbank verbleiben, werden während der Wartung aus der Datenbank gelöscht.
- **Einträge manuell löschen:** Dies ist die Standardeinstellung. Der ARP-Erkennungsverlauf wird während der Wartung nicht gelöscht.
- **Alle Einträge jetzt löschen:** Klicken Sie auf diese Schaltfläche, um den ARP-Erkennungsverlauf unverzüglich aus der Datenbank zu löschen.

Betriebssystembereitstellung

Übersicht über die Betriebssystembereitstellung

Das Extra "LANDesk Betriebssystembereitstellung" umfasst mehrere Funktionen zur Bereitstellung von Abbildern für neue oder bereits vorhandene Geräte. Diese Funktionen optimieren die Versorgung neuer Geräte und die erneute Bereitstellung vorhandener Geräte. Ferner können Sie Benutzerprofile migrieren und Abbilder mit hardwareunabhängigen Vorlagen bereitstellen, die auf verschiedene Gerätemodelle angewendet werden können.

Mit diesen automatisierten Funktionen können Sie die Bereitstellung und die erneute Bereitstellung von Abbildern für Geräte durchführen, ohne dass es hierzu eines Benutzereingriffs oder Einsatzes eines Technikers an jedem Gerät bedarf. Sie können Bereitstellungen und Migrationen so planen, dass diese nach Geschäftsschluss durchgeführt werden. Mithilfe der LANDesk® Targeted Multicast™-Technologie können Sie Netzwerkbandbreite sparen, indem Sie dasselbe Abbild auf mehreren Geräten bereitstellen.

Die folgenden Funktionen sind Teil des Extras "Betriebssystembereitstellung":

- **Betriebssystembereitstellung:** Erstellen Sie Abbilder und Skripte für die Bereitstellung von Abbildern mit Prebootumgebungen für DOS und Windows. Verwenden Sie die agenten- oder PXE-basierte Bereitstellung zur Verteilung von Abbildern.
- **Hardwareunabhängige Abbilderstellung:** Erstellen Sie eine hardwareagnostische Vorlage für die Abbilderstellung. Auf diese Weise können Sie ein und dieselbe Vorlage für Geräte von verschiedenen Herstellern verwenden. Erstellen Sie ein Repository von Treibern. Die für das jeweilige Gerät zutreffenden Treiber werden dann während des Abbilderstellungsprozesses injiziert.
- **Versorgung:** Erstellen Sie Vorlagen, mit denen eine ganze Reihe von Geräteattributen und -funktionen für den Abbilderstellungsprozess angewendet werden. Zusätzlich zur Bereitstellung von Betriebssystemabbildern können Sie Aktionen definieren, die vor und nach der Installation des Betriebssystems stattfinden, wie beispielsweise die Installation von Software, die Anwendung von Systempatches oder die Konfiguration von Laufwerks- und Netzwerkeinstellungen. Sie können neue Geräte versorgen und diese ohne Ausfallzeiten in Ihrer Umgebung einsatzbereit haben.
- **Profilmigration:** Erfassen Sie Benutzerprofildaten und stellen Sie diese wieder her, wenn Sie Computer von Benutzern aktualisieren oder Benutzern neue Computer zuweisen. Sie können den Desktop des Benutzers, die Anwendungseinstellungen, die Drucker- und Netzwerkeinstellungen sowie die Datei- und Ordnerstruktur auf dem neuen Gerät beibehalten.

Verwandte Themen

"Agentenbasierte Bereitstellung" auf Seite 393

"PXE-basierte Bereitstellung – Übersicht" auf Seite 385

"Hardwareunabhängige Abbilderstellung – Übersicht" auf Seite 399

"Versorgung (Provisioning)" auf Seite 444

"Übersicht über die Profilmigration" auf Seite 402

Verwenden der Betriebssystembereitstellung zur Bereitstellung von Abbildern

Die Funktion "Betriebssystembereitstellung" (OSD, Operating System Deployment) unterstützt zwei Methoden für die Bereitstellung von Betriebssystemabbildern auf den Geräten in Ihrem Netzwerk:

- **Agentenbasierte Bereitstellung:** Abbilder werden mit dem Windows-Betriebssystem des Geräts und den installierten LANDesk-Agenten bereitgestellt.
- **PXE-basierte Bereitstellung:** Ermöglicht das Erstellen von Abbildern für Geräte mit leeren Festplatten oder nicht funktionsfähigen Betriebssystemen. Dank der kompakten PXE-Repräsentanten benötigen Sie nicht mehr in jedem Subnetz einen fest zugeordneten PXE-Server.

Wenn Sie zum Erstellen von Abbildern das Microsoft-Dienstprogramm "Sysprep" verwenden, erstellt die Betriebssystemverteilung angepasste sysprep.inf-Dateien und fügt diese Dateien Gerät für Gerät in das Abbild des jeweiligen Geräts ein. Auf diese Weise werden der Windows-Computername, die Domäneninformationen usw. aus der Coredatenbank angepasst.

In die Betriebssystembereitstellung ist ein Abbilderstellungstool ("Imaging-Tool") integriert, mit dem Sie Abbilder erstellen können. Darüber hinaus werden Abbilderstellungstools anderer Hersteller unterstützt, die Sie u. U. bereits verwenden, z. B. Symantec Ghost, PowerQuest DeployCenter und Microsoft ImageX.

Die Betriebssystembereitstellung kann in folgenden Bootumgebungen Abbilder erstellen und Bereitstellungen sowie Migrationen durchführen:

- DOS
- Windows PE*

* Das LANDesk PE-Toolkit verwendet die Microsoft Windows Pre-installation Environment Software ("WinPE"), bei der es sich um ein Drittanbieterprodukt handelt. Damit Sie das LANDesk PE Toolkit verwenden können, müssen Sie die Microsoft WinPE-Lizenzvereinbarung akzeptiert haben.

Die Verwendung der DOS PE-Umgebung erfordert lizenzierte Software. Daher müssen Sie Kopien der lizenzierten Software bereitstellen, damit diese bei der Betriebssystembereitstellung validiert werden kann. Nur dann können Sie die DOS PE-Bootumgebung einsetzen.

WARNUNG: Gehen Sie bei der Betriebssystembereitstellung (Imaging) äußerst umsichtig vor. Die Betriebssystembereitstellung löscht alle Daten von der Festplatte eines Geräts und installiert anschließend ein neues Betriebssystem. Es besteht ein nicht zu unterschätzendes Risiko, dass wichtige Daten verloren gehen, wenn die Betriebssystembereitstellung nicht exakt den Anweisungen in diesem Dokument entsprechend ausgeführt wird oder unsachgemäß implementierte Abbilder verwendet werden. Bevor Sie eine Betriebssystembereitstellung ausführen, sollten Sie alle Daten sichern, damit verloren gegangene Daten wiederhergestellt werden können.

Schritte für die Betriebssystembereitstellung für Windows-Geräte

Planen und implementieren Sie eine Windows-Betriebssystembereitstellung mithilfe der folgenden Schritte:

1. Wenn Sie beabsichtigen, eine DOS- oder Windows PE-Imaging-Umgebung zu verwenden und Sie die Gültigkeit Ihrer Lizenzen noch nicht validiert haben, klicken Sie im Fenster **Betriebssystembereitstellung** auf die Symbolleistenschaltfläche **Lizenzen validieren**. Windows PE wird im Rahmen der Installation von Management Suite für Sie installiert. Bevor Sie die Windows PE-

Umgebung nutzen können, müssen Sie die Lizenzbedingungen akzeptieren. (Um diesen Vorgang einzuleiten, klicken Sie auf die Schaltfläche **Lizenz**. Lesen Sie vorher unbedingt den nachstehenden wichtigen Hinweis.) Für DOS PE klicken Sie auf **Jetzt validieren** und legen dann bei entsprechender Aufforderung die Betriebssystem-CDs ein. Diesen Schritt müssen Sie nur dieses eine Mal durchführen.

2. (Optional) Führen Sie den Installations-Manager von Microsoft und das Dienstprogramm Sysprep auf dem Gerät aus, dessen Abbild erstellt werden soll.
3. Erstellen Sie ein Skript für die Abbilderstellung oder verwenden Sie ein vorhandenes Skript im Fenster **Betriebssystembereitstellung**.
4. Planen Sie mit dem Extra **Geplante Tasks** einen Task, mit dem das Skript für die Abbilderstellung auf dem Gerät ausgeführt wird, dessen Abbild erstellt werden soll. (Im Fenster **Status des benutzerdefinierten Auftrags** wird angezeigt, ob dieser Task erfolgreich war oder gescheitert ist.)
5. Erstellen Sie ein Skript für die Abbildbereitstellung oder verwenden Sie ein vorhandenes Skript im Fenster **Betriebssystembereitstellung**.
6. Planen Sie mit **Geplante Tasks** einen Task, mit dem das Abbildbereitstellungsskript auf den Zielgeräten, auf denen das Abbild bereitgestellt werden soll, ausgeführt wird.
7. Zielgeräte, auf denen ein Windows-Betriebssystem und LANDesk Agenten ausgeführt werden, führen den Abbildbereitstellungsauftrag zum geplanten Zeitpunkt aus (agentenbasierte Verteilung).
8. PXE-fähige Zielgeräte führen den Abbildbereitstellungsauftrag aus, wenn sie das nächste Mal gestartet werden (PXE-basierte Bereitstellung).

WICHTIG: Dieses Produkt installiert im Rahmen der Produktinstallation Komponenten aus dem Windows Automated Installation Kit (WAIK) für Windows 7, darunter auch eine Windows PE-Umgebung. Installieren Sie keinesfalls eine andere Version des WAIK auf Ihrem Coreserver, sonst kann es zu Konflikten zwischen den beiden WAIK-Versionen kommen. Wenn Sie eine andere Version des WAIK verwenden möchten, installieren Sie diese auf einem anderen Computer als Ihrem Coreserver.

Schritte für die Betriebssystembereitstellung für Linux-Geräte

In der folgenden Liste sind die für Linux-Installationen geltenden Einschränkungen aufgeführt.

1. Die Stammpartition ('/') muss vom Dateisystemtyp ext2, ext3 oder xfs sein.
2. Die Stammpartition *darf nicht* in einem LVM PV (Logical Volume Manager - Physical Volume) enthalten sein, sondern *muss* eine Partition (physikalisch oder erweitert) im MBR (Master Boot Record) des Laufwerks sein.
3. Die letzte Partition ist die einzige Partition, die erweitert werden kann; aus diesem Grund muss auch diese Partition vom Dateisystemtyp ext2, ext3 oder xfs sein.
4. Sie müssen angeben, in welcher Partition sich die Stammpartition befindet (hda3 oder sda2)

Planen und implementieren Sie eine Linux-Betriebssystembereitstellung mithilfe der folgenden Schritte:

1. Erstellen Sie ein Abbilderstellungsskript für die Linux-Konfiguration im Fenster **Betriebssystembereitstellung** oder verwenden Sie ein vorhandenes Skript.
2. Planen Sie mit dem Extra **Geplante Tasks** einen Task, mit dem das Skript für die Abbilderstellung auf dem Gerät ausgeführt wird, dessen Abbild erstellt werden soll. (Im Fenster **Status des benutzerdefinierten Auftrags** wird angezeigt, ob dieser Task erfolgreich war oder gescheitert ist.)

3. Erstellen Sie mit dem Assistenten für **Tasks zur Betriebssystembereitstellung/Migration** ein neues Abbildbereitstellungsskript für die Linux-Konfiguration oder verwenden Sie ein vorhandenes Skript.
4. Planen Sie mit **Geplante Tasks** einen Task, mit dem das Abbildbereitstellungsskript auf den Zielgeräten, auf denen das Abbild bereitgestellt werden soll, ausgeführt wird.
5. Zielgeräte, auf denen ein Windows-Betriebssystem und LANDesk Agenten ausgeführt werden, führen den Abbildbereitstellungsauftrag zum geplanten Zeitpunkt aus (agentenbasierte Verteilung).
6. PXE-fähige Zielgeräte führen den Abbildbereitstellungsauftrag aus, wenn sie das nächste Mal gestartet werden (PXE-basierte Bereitstellung).

Richtlinien für die Erstellung von Betriebssystemabbildern

Sie können Betriebssystemabbilder mit dem LANDesk Abbilderstellungstool oder anderen Imaging-Tools erstellen. Wenn Sie den Assistenten für Tasks zur Betriebssystembereitstellung/Migration ausführen, um ein Imaging-Skript zu erstellen, werden Sie aufgefordert, den Abbildtyp und das Imaging-Tool anzugeben. Der Assistent erstellt automatisch Befehlszeilen für das LANDesk Abbilderstellungstool (ImageW) und für Microsoft ImageX, aber nicht für Symantec Ghost oder andere Abbilderstellungstools.

HINWEIS: Beim Installieren der Betriebssystembereitstellungs- und Profilmigrationskomponente werden automatisch Dateien für das LANDesk Abbilderstellungstool auf dem Coreserver installiert. Wenn Sie das LANDesk Abbilderstellungstool von einem anderen Speicherort ausführen möchten, müssen Sie die folgenden vier Dateien kopieren: imageall.exe, image.exe, restall.bat, and backall.bat. Wenn Sie Microsoft ImageX verwenden möchten, müssen Sie die Dateien imagex.exe und xmlrw.dll in den Ordner \\<Core>\ManagementSuite\OSD\imaging kopieren.

Wenn Sie mit einem anderen Abbilderstellungstool arbeiten, können Sie die Befehlszeile für dieses Tool am Ende des Assistenten angeben. Bei Angabe einer benutzerdefinierten Befehlszeile fügt der Assistent diese Zeile an der richtigen Stelle im Skript ein, und Sie müssen das Skript nicht manuell bearbeiten.

Erläuterungen zu den Imaging-Umgebungen für die Betriebssystembereitstellung

Beim Aufzeichnen oder Wiederherstellung eines Abbilds bootet die Betriebssystembereitstellung das Zielgerät in eine Imaging-Umgebung). Die Betriebssystembereitstellung unterstützt folgende Imaging-Umgebungen:

- **DOS**: Die Lizenzverifizierung erfordert eine Windows NT 4 Server- und eine Windows 98-CD. Dieses Abbild ist das kleinste Abbild und beansprucht deshalb relativ wenig Netzwerkbandbreite. Hinsichtlich der Erstellung und Wiederherstellung von Abbildern ist es unter Umständen das langsamste und auch mit weniger Hardware kompatibel als Windows PE.
- **Windows PE**: Die Lizenz ist in diesem Produkt enthalten. Dieses Abbild ist das größte. Es weist die beste Hardwarekompatibilität auf und verursacht beim Erstellen und Wiederherstellen von Abbildern den geringsten Zeitaufwand. Die Abbilderstellungsgeschwindigkeit profitiert von 32-Bit-Treibern und Anwendungen. Diese Abbilderstellungsumgebung unterstützt auch die Abbilderstellungstools von Microsoft.

Beachten Sie, dass die von Ihnen gewählte Imaging-Umgebung nicht an das Betriebssystem gebunden ist, von dem Sie ein Abbild erstellen. Es ist beispielsweise problemlos möglich, in einer Windows-Imaging-Umgebung ein Abbild von einem Linux-Betriebssystem zu erstellen.

Abbilddateinamen

Weisen Sie den Abbildern eindeutige Dateinamen zu. Wenn Sie gleichzeitig unterschiedliche Abbilder mit demselben Dateinamen im selben Subnetz bereitstellen, sind Probleme vorprogrammiert. Je nachdem, welche Namen den Abbilddateien vom Imaging-Tool zugewiesen werden, und abhängig von der verwendeten Imaging-Umgebung (z. B. Ghost-Multidateiabbilder), besitzt der Dateiname unter Umständen nur fünf eindeutige Zeichen, sobald er in ein DOS 8.3-Namensformat konvertiert wird.

Beim Aufzeichnen von Abbildern verwendet das LANDesk Abbilderstellungstool für DOS, Windows und Linux die letzten sechs Zeichen des Computernamens, gefolgt von einer zweistelligen Abbildnummer für jede Datei im Abbild. Wenn Sie Abbilder von mehreren Geräten zur selben Zeit aufzeichnen und die letzten sechs Zeichen des Computernamens nicht eindeutig sind, treten während des Aufzeichnungsvorgangs Fehler auf.

Symantec Ghost verwendet normalerweise die ersten acht Zeichen des Computernamens für den Abbilddateinamen, der auch eindeutig sein muss, damit die simultane Abbildaufzeichnung fehlerfrei abläuft.

Werden Abbilder von mehreren Geräten erstellt, gibt es zwei Möglichkeiten sicherzustellen, dass die Abbilder eindeutige Namen aufweisen:

- Erstellen Sie nacheinander von jedem Gerät ein Abbild und benennen Sie die Abbilder dabei um.
- Stellen Sie vor der Ausführung des Auftrags sicher, dass die letzten sechs Zeichen (LANDesk Abbilderstellungstool) oder die ersten acht Zeichen (Symantec Ghost) Ihrer Windows-Computernamen eindeutig sind.

LANDesk Agenten und Abbilder

Die Abbilder sollten keine LANDesk-Agenten enthalten. Wenn Sie ein Sysprep-Abbild verwenden, installiert die Betriebssystembereitstellung die LANDesk-Agenten auf dem Windows-basierten Betriebssystem, nachdem das Abbild wiederhergestellt wurde.

Wenn Ihre Windows-basierten Nicht-Sysprep-Abbilder LANDesk Agenten enthalten, müssen Sie die Datei ldiscan.cfg aus dem Root-Verzeichnis der Festplatte löschen, bevor Sie mit der Abbilderstellung beginnen. Sie müssen zudem folgende Schlüssel löschen:

- HKLM\Software\Intel\LANDesk\Common API\Unique ID
- HKLM\Software\LANDesk\Common API\Unique ID

Andernfalls besitzen alle Geräte, die das Abbild verwenden, denselben Core-Datenbankeintrag. Es gibt noch eine andere Möglichkeit: Wenn Nicht-Sysprep-Abbilder bereits LANDesk Agenten besitzen, können Sie die Option **Doppelte Kennungen ablehnen** im Dialogfeld **Doppelte Gerätekennung** aktivieren (**Konfigurieren > Dienste > Inventar > Gerätekennungen**).

Partitionen und Abbilder

Wenn die Betriebssystembereitstellung ein Abbild auf einem Zielgerät wiederherstellt, werden standardmäßig alle bereits vorhandenen Partitionen auf diesem Gerät gelöscht.

Das LANDesk Abbilderstellungstool unterstützt Abbildungen mit einzelnen oder mehreren Partitionen (bis zu vier).

Nicht-Windows-Abbilder

Mit der Betriebssystembereitstellung können Sie fast jedes Abbild bereitstellen, das vom Abbilderstellungstool unterstützt wird, nicht nur Windows-basierte Abbilder. Beim Bereitstellen von Nicht-Windows- oder Nicht-Sysprep-Abbildern müssen Sie darauf achten, nicht die Option **Abbild wird von SysPrep verarbeitet** in den Dialogfeldern "Neue Konfiguration" auszuwählen.

Validierung von Lizenzen für Imaging-Umgebungen

Beim Aufzeichnen oder Wiederherstellung eines Abbilds bootet die Betriebssystembereitstellung das Zielgerät in eine Imaging-Umgebung). Die Betriebssystembereitstellung unterstützt zwei Imaging-Umgebungen (DOS und Windows). Sie müssen Ihre Lizenz für die Verwendung der DOS PE-Umgebung validieren, und Sie müssen die Lizenz für die Windows PE-Umgebung akzeptieren, die mit diesem Produkt installiert wird.

So validieren Sie eine DOS-PE-Umgebung

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Lizenzen validieren**.
2. Klicken Sie im Abschnitt **DOS-Abbilderstellungsumgebung** auf **Jetzt verifizieren**.
3. Legen Sie eine Windows NT4 Server-Installations-CD in ein Laufwerk ein. Klicken Sie auf **Durchsuchen** und wählen Sie den Ordner \CLIENTS\MSCLIENT\DISKS auf der CD aus.
4. Klicken Sie auf **OK**. Der Validierungsprozess greift auf die Dateien auf dieser CD zu. Nach Abschluss dieses Vorgangs werden Sie aufgefordert, die nächste CD einzulegen.
5. Wenn die Aufforderung erscheint, legen Sie eine Windows 98-Installations-CD in ein Laufwerk ein. Klicken Sie auf **Durchsuchen** und wählen Sie den Ordner \WIN98 auf der CD aus.
6. Klicken Sie auf **OK**. Der Validierungsprozess wird fortgesetzt. Wenn er abgeschlossen ist, klicken Sie auf **OK**.

So akzeptieren Sie die Lizenz für die Windows PE-Umgebung

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Lizenzen validieren**.
2. Klicken Sie im Abschnitt **Windows PE-Lizenzvereinbarung** auf **Lizenz**.
3. Klicken Sie auf den Link, um die Bedingungen der WAIK-Lizenz zu akzeptieren. Im Dialogfeld "OSD-Abbilderstellungsumgebung" erscheint die Meldung "Akzeptiert".

WICHTIG: Dieses Produkt installiert im Rahmen der Produktinstallation Komponenten aus dem Windows Automated Installation Kit (WAIK) für Windows 7, darunter auch eine Windows PE-Umgebung. Installieren Sie keinesfalls eine andere Version des WAIK auf Ihrem Coreserver, sonst kann es zu Konflikten zwischen den beiden WAIK-Versionen kommen. Wenn Sie eine andere Version des WAIK verwenden möchten, installieren Sie diese auf einem anderen Computer als Ihrem Coreserver.

Auswählen einer Standard-Prebootumgebung (PE)

Mit dem Validierungsdialogfeld können Sie die Standard-Prebootumgebung (PE) für Geräte in der PXE-Warteschlange ändern. Geräte in der Warteschlange booten in die von Ihnen ausgewählte Umgebung. Es werden nur die von Ihnen validierten Bootumgebungen zur Auswahl angeboten.

1. Klicken Sie in der Symbolleiste des Extras für die Betriebssystembereitstellung auf die Schaltfläche **Lizenzen validieren**.
2. Wählen Sie in der Liste **Standard-Prebootumgebung (PE)** entweder **Linux** oder **Windows** als Ihre Standard-Prebootumgebung aus.
3. Klicken Sie auf **OK**.

Anpassen von Abbildern mit Sysprep und Setup Manager

Für die Bereitstellung von Windows 2003-, Windows XP- und Windows XP x64 Edition-Abbildern können Sie die Dienstprogramme "Setup Manager" und "Sysprep" von Microsoft verwenden. Sysprep passt eine Windows-Installation so an, dass beim Neustart des Betriebssystems nach einer Antwortdatei (sysprep.inf) gesucht wird und sich das Betriebssystem selbst für das neue Gerät konfiguriert. Setup Manager erstellt die sysprep.inf-Antwortdatei, die Sysprep verwendet.

Bevor Sie Skripte für die Betriebssystembereitstellung erstellen, sollten Sie Setup Manager von Microsoft (setupmgr.exe) ausführen und eine setupmgr.exe-Antwortdatei für die bereitgestellten Abbilder erstellen. Sie können diese Datei anschließend als Grundlage für von Ihnen erstellte Betriebssystembereitstellungsskripte verwenden, indem Sie die Option **Vorhandene sysprep.inf-Datei als Vorlage verwenden** auf der Assistentenseite **Sysprep-Dateiinformationen angeben** auswählen. Alle Einstellungen, die Sie im Assistenten für Betriebssystembereitstellungsskripte eingeben, überschreiben die entsprechenden Optionen in der sysprep.inf-Vorlagendatei.

Wenn Sie Sysprep für Windows 2000/XP-Abbilder verwenden, kann die Betriebssystembereitstellung eine Core-Datenbankabfrage nach den von Ihnen bereitgestellten Geräten erstellen und bestimmte Benutzereinstellungen migrieren, z. B.:

- Windows-Computername
- GUID (der eindeutige Bezeichner, mit dem Geräte in der Coredatenbank identifiziert werden)

Sie können auch die folgenden Optionen global für bereitzustellende Abbilder festlegen:

- Zeitzone
- Datenträgerlizenzschlüssel
- Registrierter Name und Organisation
- Arbeitsgruppe/Domäne/LDAP-Organisationseinheit

Die Betriebssystembereitstellung erstellt mithilfe von Informationen aus der Coredatenbank und aus dem Skript für die Abbildbereitstellung für jedes Gerät, von dem Sie ein Abbild erstellen, eine benutzerdefinierte sysprep.inf-Datei. Anschließend wird die sysprep.inf-Datei von der Betriebssystembereitstellung in das Abbild des jeweiligen Geräts eingefügt.

Zusätzliche Informationen

Nähere Informationen zu Setup Manager und zu Sysprep finden Sie auf der Microsoft Website in der Dokumentation zu den Dienstprogrammen Setup Manager und Sysprep. Sysprep umfasst zahlreiche leistungsstarke Funktionen, die nicht in diesem Dokument beschrieben werden.

Hilfestellung bei der Lösung von Problemen im Zusammenhang mit der Verwendung von Sysprep können Sie auch auf der Website der LANDesk Support Community unter community.landesk.com finden.

Erstellen eines Sysprep-Abbildes

1. Um das Gerät, dessen Abbild erstellt werden soll, auf die Abbilderstellung vorzubereiten, nehmen Sie die erforderlichen Konfigurationsänderungen oder Anpassungen vor.
2. Erstellen Sie einen Ordner c:\sysprep im Root-Verzeichnis der Festplatte des Geräts.
3. Öffnen Sie von einer Windows 2000- oder Windows XP-Installations-CD aus \Support\Tools\DEPLOY.CAB und kopieren Sie **sysprep.exe** und **setupcl.exe** in den erstellten sysprep-Ordner.
4. Öffnen Sie eine DOS-Eingabeaufforderung und wechseln Sie zum sysprep-Ordner. Führen Sie Sysprep aus. Wenn Sie nicht die Neustartoption verwenden, müssen Sie das Gerät über das Startmenü herunterfahren, sobald Sie zum Herunterfahren aufgefordert werden.
5. Starten Sie im DOS-Modus und führen Sie das Abbilderstellungstool manuell aus.

PXE-basierte Bereitstellung – Übersicht

Die Betriebssystembereitstellung unterstützt PXE-Starts und die Bereitstellung von Abbildern. Mit PXE-basierter Bereitstellung können Sie sowohl neue als auch vorhandene PXE-fähige Geräte starten und entweder über ein benutzerdefiniertes PXE-DOS-Startmenü ein Skript für die Betriebssystembereitstellung auf dem Gerät ausführen oder Geräte in die Coredatenbank scannen und anschließend mit dem Extra **Geplante Tasks** eine Abbildbereitstellung planen.

Die PXE-basierte Bereitstellung bietet in verschiedenen Situationen eine hilfreiche Methode zur Erstellung von Geräteabbilder:

- Anfängliche Bereitstellung neuer Geräte
- Erstellen von Geräteabbildern in einer Test- oder Schulungsumgebung
- Erneutes Abbilden von defekten Geräten

LANDesk Management Suite bietet mehrere Optionen, die eine Verwendung von PXE zum Bereitstellen von Betriebssystemabbildern ermöglichen:

- von LANDesk gesteuertes Starten mit der Möglichkeit, Geräte vorab als Ziele für die Abbilderstellung zu wählen
- ein PXE-Boot-Menü, in dem Sie interaktiv eine Option für ein Gerät auswählen können
- eine PXE-Warteschlange, zu der automatisch Geräte hinzugefügt werden, wenn diese einen PXE-Start durchlaufen

Grundlegendes zum PXE-Protokoll

PXE (Preboot Execution Environment) ist ein nach dem Industriestandard entwickeltes Netzwerkprotokoll, mit dem Geräte über das Netzwerk gestartet und abgebildet werden können. Dazu wird eine ausführbare Abbilddatei von einem Abbildserver heruntergeladen und installiert, bevor das Gerät von der lokalen Festplatte gestartet wird. Auf einem PXE-fähigen Gerät wird das PXE-Protokoll entweder aus dem Flash- bzw. ROM-Speicher des Netzwerkadapters oder aus dem System-BIOS geladen.

PXE verwendet folgende Kommunikationsstandards:

- DHCP (Dynamic Host Configuration Protocol)
- TFTP (Trivial File Transfer Protocol)
- MTFTP (Multicast Trivial File Transfer Protocol)

Beim Start eines PXE-fähigen Geräts wird eine DHCP-Erkennungsanforderung übertragen. Wenn ein DHCP-Server erkannt wird, der PXE implementiert, weist der Server dem Gerät eine IP-Adresse zu und sendet Informationen zu verfügbaren PXE-Startservern. Wenn der DHCP-Erkennungsprozess abgeschlossen ist, kontaktiert das Gerät den PXE-Server und downloadet über TFTP eine Abbilddatei. Anschließend wird das Abbilderstellungsskript ausgeführt, mit dem das Betriebssystemabbild vom Abbilderstellungsserver auf das Gerät geladen wird. Auf die Abbilddatei wird mit einem Betriebssystembereitstellungsskript verwiesen.

Weitere Informationen zu PXE und den zugrunde liegenden Technologien und Funktionen finden Sie in der PXE-Spezifikation v2.1 unter http://download.intel.com/design/archives/wfm/downloads/pxespec.pdf.

Übersicht über die PXE-Konfiguration mit Management Suite

Die folgende Liste bietet eine Übersicht über den Prozess, den Sie durchführen müssen, um auf den von Ihnen verwalteten Geräten die PXE-Startfunktion verwenden zu können.

1. Stellen Sie sicher, dass Ihre OSD-Umgebung für DOS- oder Windows PE-Imaging validiert wurde. Um dies zu prüfen, klicken Sie zunächst auf **Konfigurieren > Dienste** und dann auf der Registerkarte **Allgemein** auf die Schaltfläche **OSD-Validierung**. Die Abbilderstellung, die Sie in Verbindung mit der PXE-Startfunktion verwenden, muss mit dem Betriebssystem übereinstimmen, das validiert wurde.
2. Erstellen Sie ein OSD-Konfigurationsskript zur Erfassung eines Abbilds. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung** und wählen Sie dann in der Symbolleiste den PE-Typ aus, den Sie verwenden werden. Sie müssen die Skripte erstellen, die Sie Benutzern im PXE-Startmenü zur Verfügung stellen wollen.
3. Fügen Sie Skripte zum PXE-Startmenü hinzu. Klicken Sie auf **Extras > Verteilung > PXE-Startmenü**. Ziehen Sie Skripte aus dem Fenster "Betriebssystembereitstellung" auf das Fenster "PXE-Boot-Menü" und ordnen Sie die Skripte dann in der Reihenfolge, in der sie im PXE-Menü erscheinen sollen.
4. Stellen Sie auf jedem Subnetz, auf dem PXE-Boot verfügbar sein soll, einen PXE-Repräsentanten bereit. Ein Skript für die PXE-Repräsentantenbereitstellung befindet sich im Ordner **Alle anderen Skripte**. (Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung > OSD-Skripte > Alle anderen Skripte**).
5. Richten Sie PXE-fähige Geräte entsprechend den von Ihnen bevorzugten Neustartoptionen ein: Wählen Sie entweder einen Netzwerkstart zur Startzeit oder richten Sie das BIOS so ein, dass das Gerät zuerst vom Netzwerk startet.
6. Wenn Sie ein PXE-fähiges Gerät neu starten, drücken Sie **F8**, um das PXE-Boot-Menü zu öffnen. Wählen Sie die Bootoption aus, die Sie auf dieses Gerät anwenden wollen.

Neustart von Geräten mit einem PXE-Boot-Menü

Wenn ein PXE-fähiges Gerät gestartet wird, passiert Folgendes:

1. Das PXE-fähige Gerät sendet eine Abfrage für PXE-Dienste, die auf einem PXE-Repräsentanten im Netzwerk ausgeführt werden.
2. Wenn es in dem betreffenden Subnetz einen PXE-Repräsentant gibt, antwortet dieser und weist das Gerät an, den Startvorgang mit PXE fortzusetzen.
3. Auf dem Gerät wird eine PXE-Startsitzung initiiert und die Eingabeaufforderung für den PXE-Start angezeigt. Die Standardeingabeaufforderung lautet "Drücken Sie F8, um das Menü anzuzeigen." und wird vier Sekunden lang angezeigt. (Sie können die Einstellungen für diese PXE-Eingabeaufforderung auf der Registerkarte **Konfigurieren > Dienste > Betriebssystembereitstellung** ändern.)

4. Wenn Sie die Taste **F8** vor Ablauf des Zeitintervalls drücken, wird ein vorläufiges PXE-Startmenü angezeigt, in dem Sie folgende Startoptionen auswählen können:

    - **Lokales Starten:** Das Gerät wird über die lokale Festplatte gestartet. Wenn kein Betriebssystem vorhanden ist, wird eine Fehlermeldung ausgegeben.
    - **Von LANDesk gesteuertes Starten:** Das Gerät wird in die Netzwerkansicht der Konsole eingefügt (die MAC-Adresse des Geräts wird angezeigt); von dort können Sie die Ausführung eines Betriebssystembereitstellungsskripts auf dem Gerät planen.
    - **LANDesk Startmenü:** Das Gerät zeigt das Startmenü an, das Sie mit dem Extra "PXE-Boot-Menü" erstellt haben. Sie können ein Betriebssystembereitstellungsskript auswählen und auf dem Client ausführen.

5. Wenn die Taste **F8** nicht vor Ablauf des Zeitintervalls gedrückt wird, verwendet das Gerät die Standard-Startoption. Die standardmäßige Startoption hängt von folgenden Bedingungen ab:

    - Wenn das Gerät einen geplanten Abbilderstellungsauftrag für sich in der Coredatenbank ermittelt (entweder ein fehlgeschlagener oder anstehender Auftrag), wird ein von LANDesk**gesteuertes Starten** als standardmäßige Startoption verwendet.
    - Wenn das Gerät *keinen* Abbildauftrag für sich ermittelt, wird standardmäßig **Lokales Starten** verwendet.
    - Das PXE DOS-Menü wird nie als Standard-Startoption eingestellt.

6. Das geplante Betriebssystembereitstellungsskript wird auf dem Gerät ausgeführt.

Verwandte Themen

"Konfigurieren der Eingabeaufforderung für den PXE-Start" auf Seite 390

"Verwenden des PXE-Startmenüs" auf Seite 391

Verwenden von PXE-Repräsentanten

Die PXE-Unterstützungssoftware wird im Rahmen der Standardinstallation der Betriebssystembereitstellung auf dem Coreserver installiert. Um die PXE-Unterstützung zu aktivieren, müssen Sie jedoch zunächst PXE-Einstellungen konfigurieren und dann einen PXE-Repräsentanten in jedem Subnetz des Netzwerks bereitstellen, das PXE-Unterstützung bieten soll. PXE-Repräsentanten sorgen für Skalierbarkeit im Netzwerk, da sie Betriebssystemabbilder auf Geräten in ihren jeweiligen Subnetzen bereitstellen.

Die Geräte in den Subnetzen verwenden normale PXE-Abfragen und Dateiübertragungsmethoden, um mit dem vorhandenen PXE-Repräsentanten zu kommunizieren, der wiederum mithilfe von Webdiensten (HTTP) mit dem Coreserver kommuniziert.

HINWEIS: Deaktivieren von anderen PXE-Servern
Falls derzeit irgendein anderer PXE-Server im Netzwerk ausgeführt wird, müssen Sie diesen zuerst deaktivieren, um die LANDesk PXE-Unterstützung nutzen zu können.

Bereitstellen von PXE-Repräsentanten

Sie müssen in jedem Subnetz, in dem Sie PXE-Boot-Unterstützung zur Verfügung stellen möchten, einen PXE-Repräsentanten bereitstellen. Um einen PXE-Repräsentanten einzurichten, müssen Sie das PXE-Repräsentantenbereitstellungsskript auf dem ausgewählten Gerät ausführen. Dieses vordefinierte Skript wird im Extra **Skripte verwalten** bereitgestellt. (Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung > OSD-Skripte**, und klicken Sie dann auf den Ordner **Alle anderen Skripte**.)

Zur Unterstützung der Lastverteilung werden in einem Subnetz mehrere PXE-Repräsentanten unterstützt. In diesem Fall wird der erste PXE-Repräsentant, der auf eine Geräteanforderung antwortet, für die Kommunikation mit dem Coreserver verwendet.

HINWEIS: Auf dem Coreserver sollte *kein* PXE-Repräsentant bereitgestellt werden.

Das als PXE-Repräsentant ausgewählte Gerät muss keine speziellen Hardwareanforderungen erfüllen. Es gelten jedoch folgende Softwareanforderungen:

- **Betriebssystem:** Windows 2000 Professional SP4, Windows XP SP3, Windows Vista SP2, Windows 7, Windows Server 2000 SP4, Windows Server 2003 SP2 oder Windows Server 2008.

  Bei Windows 2000 müssen Sie sicherstellen, dass der Microsoft-MSI-Dienst ausgeführt wird (XP umfasst MSI standardmäßig). Wenn der neueste Service Pack installiert ist, wird der MSI-Dienst im Normalfall ausgeführt. Andernfalls können Sie ihn folgendermaßen über die Konsole auf dem PXE-Repräsentanten bereitstellen: Klicken Sie auf **Extras > Verteilung > Skripte verwalten**, wählen Sie den Task **MSI service deployment** (MSI-Dienstbereitstellung) unter **Alle Skripte** und klicken Sie auf die Schaltfläche **Planen**. Ziehen Sie in den Fenstern **Geplante Tasks** die Zielgeräte in das Fenster, klicken Sie mit der rechten Maustaste auf den Task **MSI service deployment** (MSI-Dienstbereitstellung) und wählen Sie **Eigenschaften**, klicken Sie auf **Task planen** und geben Sie eine Startzeit ein, um die Bereitstellung des MSI-Dienstes zu planen.

- **Installierte LANDesk Agenten:** Softwareverteilungs-Agent und Inventarscanner-Agent. Weitere Informationen finden Sie unter "Agentenkonfiguration" auf Seite 105".

Aktualisieren von PXE-Repräsentanten

Wenn Sie die Einstellungen für die PXE-Startoption ändern (unter Konfigurieren > Dienste > Betriebssystembereitstellung), müssen Sie alle PXE-Repräsentanten aktualisieren, indem Sie das Skript "PXE-Repräsentantenbereitstellung" erneut ausführen, damit die Änderungen für die PXE-Repräsentanten der einzelnen Subnetze übernommen werden. Die erneute Ausführung des Skripts ist jedoch nicht erforderlich, wenn Sie die PXE-Proxys nur aus der Liste "Verfügbare Proxys" in die Liste "Warteschlangen-Proxys" verschieben.

Aktualisieren von Windows PE-Abbilder

Wenn Sie ein Windows PE-Abbild in irgendeiner Weise ändern, müssen die von Ihnen vorgenommenen Änderungen auf all PXE-Repräsentanten übertragen werden. Dies geschieht normalerweise durch eine erneute Bereitstellung der PXE-Repräsentanten und kann sowohl Bandbreite als auch Zeit in Anspruch nehmen. Informationen zur Skripten, die Sie verwenden können, um das aktualisierte Windows PE-Abbild einfach auf alle PXE-Repräsentanten zu kopieren, finden Sie in folgendem Dokument in der LANDesk Benutzercommunity:

http://community.landesk.com/support/docs/DOC-7619

Bereitstellen eines PXE-Repräsentanten

Sie müssen in jedem Subnetz, in dem Sie PXE-Boot-Unterstützung zur Verfügung stellen möchten, einen PXE-Repräsentanten bereitstellen. Um einen PXE-Repräsentanten einzurichten, müssen Sie das PXE-Repräsentantenbereitstellungsskript auf dem ausgewählten Gerät ausführen.

So stellen Sie einen PXE-Repräsentanten bereit

1. Klicken Sie in der Konsole auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** auf das Strukturelement **Alle anderen Skripte**. Klicken Sie auf das Skript **PXE Representative deployment** (PXE-Repräsentantenbereitstellung) und anschließend in der Symbolleiste auf die Schaltfläche **Planen**.
3. Wählen Sie in der Netzwerkansicht der Konsole das Zielgerät aus, auf dem die PXE-Dienste installiert werden soll.
4. Verschieben Sie das ausgewählte Gerät mit Ziehen und Ablegen auf den Task **PXE Representative deployment** (PXE-Repräsentantenbereitstellung) im Fenster **Geplante Tasks**.
5. Klicken Sie mit der rechten Taste auf **PXE Representative deployment** (PXE-Repräsentantenbereitstellung), klicken Sie dann auf **Eigenschaften** und schließen Sie den Konfigurationsvorgang für den Task ab.

Aktualisieren oder Entfernen von PXE-Repräsentanten

Wenn Sie die Einstellungen für die PXE-Startoption ändern (unter **Konfigurieren > Dienste > Betriebssystembereitstellung**), müssen Sie alle PXE-Repräsentanten aktualisieren, indem Sie das Skript "PXE Representative Deployment" (PXE-Repräsentanten bereitstellen) erneut ausführen, damit die Änderungen für die PXE-Repräsentanten der einzelnen Subnetze übernommen werden.

Das Verfahren ist ähnlich, wenn Sie die Verwendung eines Geräts als PXE-Repräsentanten einstellen. Sie führen in diesem Fall das Skript "PXE Representative Removal" (PXE-Repräsentanten entfernen) aus, um dieses Gerät aus den PXE-Repräsentanten in Ihrem Netzwerk zu entfernen.

So aktualisieren Sie PXE-Repräsentanten

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie auf **Alle anderen Skripte** und klicken Sie dann auf **PXE Representative Deployment**. Klicken Sie mit der rechten Maustaste auf das Skript und wählen Sie **Planen** aus.
3. Fügen Sie die ausgewählten Geräte mittels Ziehen und Ablegen in die entsprechenden Tasks im Fenster **Geplante Tasks** ein.
4. Klicken Sie mit der rechten Taste auf den Task, klicken Sie auf **Eigenschaften** und schließen Sie den Konfigurationsvorgang für den Task ab.

Die erneute Ausführung des Skripts ist jedoch nicht erforderlich, wenn Sie die PXE-Proxies nur aus der Liste "Verfügbare Proxies" in die Liste "Warteschlangen-Proxies" verschieben.

So entfernen Sie PXE-Repräsentanten

1. Klicken Sie auf **Extras > Verteilung > Skripte verwalten**.
2. Klicken Sie auf **Alle anderen Skripte** und klicken Sie dann auf **PXE Representative Removal**. Klicken Sie mit der rechten Maustaste auf das Skript und wählen Sie **Planen** aus.

3. Fügen Sie die ausgewählten Geräte mittels Ziehen und Ablegen in die entsprechenden Tasks im Fenster **Geplante Tasks** ein.
4. Klicken Sie mit der rechten Taste auf den Task, klicken Sie auf **Eigenschaften** und schließen Sie den Konfigurationsvorgang für den Task ab.

Konfigurieren der Eingabeaufforderung für den PXE-Start

Sie können das Verhalten der PXE-Start-Eingabeaufforderung steuern, die beim Versuch eines PXE-Starts durch das Gerät angezeigt wird.

Beim Starten eines PXE-fähigen Geräts versucht eine DHCP-Anforderung eine PXE-Sitzung zu initiieren, indem sie nach einem Server (oder Proxy) sucht, auf dem die PXE-Dienst-Software (PXE- und MTFTP-Dienste) ausgeführt wird. Wenn das Gerät einen PXE-Server entdeckt, wird auf dem Gerät einige Sekunden lang die Eingabeaufforderung für den PXE-Start angezeigt. Wenn Sie vor Ablauf des Zeitintervalls die Funktionstaste F8 drücken, können Sie auf das PXE-Startmenü zugreifen und ein Betriebssystemabbild auswählen, um es auf dem Gerät bereitzustellen.

So konfigurieren Sie Optionen der Eingabeaufforderung für den PXE-Start

1. Klicken Sie auf **Konfigurieren > Dienste** und klicken Sie dann auf die Registerkarte **Betriebssystembereitstellung**.
2. Geben Sie einen Wert (in Sekunden) in das Feld **Timeout** ein. Standardmäßig werden 4 Sekunden verwendet. Es können maximal 60 Sekunden eingegeben werden.
3. Geben Sie eine Meldung in das Textfeld **Meldung** ein. Standardmäßig wird die Meldung "Drücken Sie F8, um das Menü anzuzeigen" angezeigt. Es können maximal 75 Zeichen eingegeben werden.
4. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern, oder auf **OK**, um die Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn auf den Subnetzen Ihres Netzwerks PXE-Repräsentanten ausgeführt werden, sollten Sie die für die PXE-Start-Eingabeaufforderung vorgenommenen Änderungen für diese Proxies implementieren, indem Sie sie aktualisieren. Zu diesem Zweck planen Sie das PXE-Repräsentantenbereitstellungsskript zu Ausführung auf allen Geräten, die PXE-Repräsentanten sind.

Verwenden des von LANDesk gesteuerten Startens

"Von LANDesk gesteuertes Starten" ist die Standardoption für das Starten, wenn ein PXE-fähiges Gerät startet und für sich ein fehlgeschlagenes Skript für die Abbildbereitstellung oder für einen fehlgeschlagenen DOS-Task in der Coredatenbank ermittelt. Sie können diese Startoption auch manuell auf dem Gerät auswählen, wenn das Startoptionsmenü angezeigt wird.

Da mit "Von LANDesk gesteuertes Starten" unbeaufsichtigte Bereitstellungen möglich sind, eignet sich diese Option, um bereits vorab Zielgeräte für die Abbilderstellung anzugeben. So können Sie beispielsweise vor dem Einfügen neuer Geräte in ein Netzwerk ein bestimmtes Betriebssystemabbild für diese Geräte angeben, indem Sie eine .CSV-Datei, die MAC-Adressen von Geräten beinhaltet, in die Coredatenbank importieren.

So geben Sie vorab Zielgeräte mit der Option "Von LANDesk gesteuertes Starten" an

1. Bevor die PXE-fähigen Geräte in das Netzwerk integriert werden, fügen Sie ihre Identifikationen durch Importieren einer .CSV-Datei in die Coredatenbank ein.
2. Planen Sie einen Abbildbereitstellungsauftrag für die Geräte. Der Abbilderstellungsauftrag misslingt, weil die Geräte noch nicht mit dem Netzwerk verbunden sind.
3. Fügen Sie die Geräte in das Netzwerk ein und starten Sie sie.

4. Die Geräte erkennen einen fehlgeschlagenen Abbilderstellungsauftrag und verwenden standardmäßig die Option "Von LANDesk gesteuertes Starten".
5. Der zuvor fehlgeschlagene Abbildbereitstellungsauftrag wird automatisch ausgeführt und für die Zielgeräte ein Abbild erstellt.

Verwenden des PXE-Startmenüs

Mit dem PXE-Startmenü können Sie ein Abbildbereitstellungsskript interaktiv für ein Gerät auswählen, ohne einen Abbildbereitstellungsauftrag planen zu müssen. Diese Methode ist nützlich, wenn für beschädigte Geräte neue Abbilder erstellt werden müssen. Bevor Sie das PXE-Startmenü verwenden, müssen Sie es zunächst konfigurieren, indem Sie die Betriebssystembereitstellungsskripte hinzufügen, die im Menü angezeigt werden sollen.

Sie erstellen das PXE-Startmenüsystem, indem Sie Verzeichnisse erstellen und vorkonfigurierte Betriebssystembereitstellungsskripte in diesen Verzeichnissen ablegen. Die Skriptbeschreibung wird als Menüelement im PXE-Startmenü des Geräts angezeigt.

So konfigurieren Sie das PXE-Startmenü

1. Klicken Sie auf **Extras > Verteilung > PXE-Startmenü**.
2. Um ein neues Verzeichnis oder Unterverzeichnis in das Menüsystem einzufügen, klicken Sie auf die Symbolleistenschaltfläche **Neu**.
3. Geben Sie einen Namen für das Verzeichnis ein. Im Verzeichnisnamen kann beispielsweise die Betriebssystemplattform oder Versionsnummer der im Verzeichnis enthaltenen Abbilder wiedergegeben werden. Sie können den Verzeichnisnamen jederzeit ändern, indem Sie in der Symbolleiste auf die Schaltfläche **Umbenennen** klicken.
4. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung** und fügen Sie die Skripte für die Betriebssystembereitstellung mittels Ziehen und Ablegen in das entsprechende Verzeichnis im Fenster **PXE-Boot-Menü** ein.
5. Um das PXE-Startmenü zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Update**.

Sie müssen in der Konsole auf die Schaltfläche **Update** klicken, wenn die Änderungen beim Starten im PXE-Startmenü auf PXE-Geräte angezeigt werden sollen.)

Das übergeordnete Verzeichnis kann bis zu vier Unterverzeichnisebenen besitzen. In jedem Verzeichnis können maximal 18 Skripte abgelegt werden.

Zugriff auf das PXE-Startmenü von einem Gerät aus

1. Starten Sie ein PXE-fähiges Gerät.
2. Wenn die Eingabeaufforderung für den PXE-Start angezeigt wird, drücken Sie vor Ablauf des Zeitintervalls die Funktionstaste **F8**.
3. Wählen Sie **PXE-DOS-Menü**. Das Menüsystem, das Sie im Fenster "PXE-Startmenü" der Konsole konfiguriert haben, wird angezeigt.
4. Um ein Verzeichnis zu öffnen und seine Unterverzeichnisse und Abbilder anzuzeigen, geben Sie die Verzeichnisnummer ein und drücken die **Eingabetaste**. Navigieren Sie im Menüsystem und suchen Sie nach dem Abbild, das auf dem Gerät bereitgestellt werden soll. Sie können **B** drücken, um eine Ebene zurückzugehen, oder **X**, um das Menüsystem zu beenden.

5. Um ein Betriebssystemabbild (auf das in einem Betriebssystembereitstellungsskript verwiesen wird) auszuwählen, geben Sie die Nummer des Skripts ein und drücken die **Eingabetaste**. Das Skript wird ausgeführt und das Abbild auf das Gerät geladen.

Wenn Sie das Menüsystem beenden, ohne eine Auswahl zu treffen, wartet das Gerät auf einen geplanten Abbildverarbeitungsauftrag vom Coreserver.

Verwandte Themen

"PXE-basierte Bereitstellung – Übersicht" auf Seite 385

"Verwenden des PXE-Startmenüs" auf Seite 391

Verwenden der PXE-Warteschlange

Die PXE-Warteschlange ist eine weitere Methode zur Remotebereitstellung von Betriebssystemabbildern auf PXE-kompatiblen Geräten. In folgenden Situationen ist diese Methode nützlich:

- In einer gesteuerten Testumgebung, in der die Abbilder aller Geräte häufig durch identische Abbilder ersetzt werden müssen.
- Für die Abbilderstellung für "Bare-Metal"-Geräte in einer Testumgebung, die anschließend in ihre Produktionsumgebung übernommen werden können.

Wenn Sie den PXE-Repräsentanten eines Subnetzes als PXE-Warteschlange angeben, werden alle PXE-fähigen Geräte in diesem Subnetz automatisch in die PXE-Warteschlange in der Netzwerkansicht der Konsole eingefügt, sobald der PXE-Start erfolgt. Sie können ein Gerät auch zu einer PXE-Warteschlange hinzufügen, indem Sie das Skript **Zu PXE-Warteschlange hinzufügen** auf dem Gerät planen, oder indem Sie das Gerät in der Netzwerkansicht direkt in die Gruppe "PXE-Warteschlange" kopieren. Anschließend kann für die Geräte ein Abbildbereitstellungsauftrag geplant werden.

So konfigurieren Sie eine PXE-Warteschlange

1. Richten Sie PXE-Repräsentanten im Netzwerk ein.
2. Klicken Sie auf **Konfigurieren > Dienste** und klicken Sie dann auf die Registerkarte **Betriebssystembereitstellung**.
3. Wählen Sie die PXE-Repräsentanten aus und verschieben Sie sie aus der Liste **Verfügbare Proxies** in die Liste **Warteschlangen-Proxies**.

   Die Liste **Verfügbare Proxies** enthält alle im Netzwerk vorhandenen PXE-Repräsentanten; sie werden mit ihrem Gerätenamen angegeben. Diese Liste wird mithilfe des Inventarscanners generiert, mit dem die auf dem Gerät ausgeführte PXE-Software (PXE- und MTFTP-Protokolle) ermittelt wird. Der Inventarscanner wird automatisch ausgeführt, wenn ein PXE-Repräsentant erstmals eingerichtet wird.
4. Klicken Sie auf **Zurücksetzen**.

   Damit bewirken Sie, dass alle PXE-fähigen Geräte, die sich im selben Subnetz wie der ausgewählte PXE-Repräsentant befinden, wieder in die PXE-Warteschlange in der Netzwerkansicht der Konsole eingefügt werden. Für diese Geräte kann dann ein Abbilderstellungsauftrag geplant werden. Die Schaltfläche "Zurücksetzen" wird aktiviert, wenn Sie einen PXE-Repräsentanten in der Liste **Warteschlangen-Proxies** auswählen.
5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern und das Dialogfeld zu schließen.

Wenn das nächste Mal ein Gerät in diesem Subnetz gestartet wird, wird es in das Objekt "PXE-Warteschlange" in der Netzwerkansicht der Konsole eingefügt.

Bereitstellen eines Abbilds auf einem Gerät in der PXE-Warteschlange

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie auf auf einen Skript für die Betriebssystembereitstellung und klicken Sie anschließend in der Symbolleiste auf die Schaltfläche **Planen**.
3. Öffnen Sie in der Netzwerkansicht der Konsole den Ordner **PXE-Warteschlange** und wählen Sie die Zielgeräte aus, auf denen Sie das Abbild bereitstellen möchten.
4. Fügen Sie die ausgewählten Geräte mittels Ziehen und Ablegen in das Fenster **Geplante Tasks** ein. Klicken Sie mit der rechten Taste auf den Task, klicken Sie auf **Eigenschaften** und schließen Sie den Konfigurationsvorgang für den Task ab.

Agentenbasierte Bereitstellung

Mit der agentenbasierten Bereitstellung können Sie Betriebssystemabbilder auf Geräten bereitstellen, auf denen Windows 98, Windows 2000 oder Windows XP ausgeführt wird.

Voraussetzungen

Wenn Sie Abbilder nicht mittels PXE bereitstellen, müssen die Geräte folgende Kriterien erfüllen:

- Sie müssen sich in der Coredatenbank befinden, wenn Multiprozessorabbilder vorliegen.
- Standard LANDesk Agent, Enhanced Software Distribution Agent und Inventaragent müssen geladen sein. Die Betriebssystembereitstellung verwendet den Softwareverteilungsagenten für die Verteilung von Abbildern.

Was geschieht während einer agentenbasierten Bereitstellung?

1. Der Coreserver stellt eine Verbindung zum Gerät her und führt alle Vorkonfigurationsbefehle aus, die Sie im Abbildbereitstellungsskript angegeben haben.
2. Die Betriebssystembereitstellung verwendet den Softwareverteilungsagenten, um eine virtuelle Bootpartitions-Datei an das Gerät zu verteilen. Außerdem wird der Bootsektor bearbeitet, damit von dieser Datei gebootet wird; anschließend wird das Gerät neu gestartet.
3. Das Gerät startet im DOS-oder Windows PE-Modus (je nachdem, was ausgewählt wurde), ermittelt und lädt einen Netzwerktreiber, bevor es die Abbilddatei vom Abbildserver abruft und installiert.

   Bei Nicht-Sysprep-Abbildern startet das Gerät nach Abschluss der Abbildverarbeitung neu. Die Betriebssystem-Bereitstellung betrachtet den Auftrag nach diesem Neustart als abgeschlossen.

   Bei Sysprep-Abbildern wird die agentenbasierte Bereitstellung folgendermaßen fortgesetzt:

4. Vor dem Neustart und dem Laden des Abbilds ersetzt der DOS- oder Windows PE-Agent die Datei sysprep.inf durch eine für dieses Gerät angepasste Datei.
5. Das abgebildete Gerät wird gestartet und passt sich entsprechend den Einstellungen in der sysprep.inf-Datei an.
6. Für Windows-Abbilder werden alle Befehle, die Sie nach der Abbilderstellung im Abbilderstellungsskript angegeben haben, über den Registrierungsschlüssel "RunOnce" ausgeführt.

7. Für Windows-Abbilder führt die Betriebssystembereitstellung die Datei wscfg32.exe unter Verwendung Ihrer Standardkonfiguration für Geräteagenten aus, um die LANDesk Agenten neu zu installieren.

Verwenden von Targeted Multicast zur Bereitstellung von Skripten

In diesem Abschnitt wird beschrieben, wie Abbilder mit der LANDesk® Targeted Multicast™-Technologie bereitgestellt werden. Multicasting ist zeitaufwendiger als Einzelverteilungen. Multicasting benötigt weniger Bandbreite und stellt das Abbild auf der Festplatte des Zielgeräts zur Verfügung. Bei vier oder mehr Geräten lohnt sich der Einsatz von Multicasting jedoch, weil dann genügend Bandbreite eingespart wird.

Targeted Multicast unterstützt Abbilder mit Einzelpartitionen, aber keine Abbilder mit mehreren Partitionen. Wenn Sie Targeted Multicast für die Betriebssystembereitstellung verwenden, können Abbilder bis zu zehn Dateien umfassen.

Beim Multicasting von Abbildern wird die Abbilddatei im Zwischenspeicher des Geräts abgelegt, bevor sie wiederhergestellt wird. Auf der Festplatte des Geräts muss genügend Speicherplatz für die Abbilddatei und die wiederhergestellten Dateien vorhanden sein.

Bevor Sie Multicasting für die Betriebssystembereitstellung verwenden, müssen Sie sicherstellen, dass sich die Multicasting-Komponenten in dem Subnetz befinden, an das die Abbilddateien verteilt werden sollen. Multicast-Betriebssystembereitstellungen misslingen u. U., wenn Sie nicht für jede Multicast-Domäne in der Gruppe **Multicast-Domänenrepräsentanten** der Netzwerkansicht einen Domänenrepräsentanten angeben. Die Verwendung von Targeted Multicasting setzt voraus, dass Sie auf den Geräten LANDesk Management Suite Agenten ab Version 6.62 und im Subnetz einen LANDesk Management Suite Multicast-Domänenrepräsentanten ab Version 6.62 installiert haben.

Wenn Sie Dateien mithilfe von Multicast an ein Subnetz verteilen möchten, das keinen Multicast-Domänenrepräsentanten besitzt, wird die Bereitstellung zwar gestartet, jedoch nicht abgeschlossen. Sie müssen eine Startdiskette für die Betriebssystembereitstellung erstellen, um die Geräte manuell zu starten.

Wenn die Router UDP-Broadcasts weiterleiten und es im Subnetz, das das verteilte Abbild erhält, Windows-Geräte gibt, die als Multicast-Domänenrepräsentant fungieren, kann Targeted Multicast verwendet werden, ohne dass Multicast-Domänenrepräsentanten angegeben werden müssen.

Wenn die Router keine UDP-Broadcasts weiterleiten, müssen Sie die Multicast-Domänenrepräsentanten manuell für jedes Subnetz auswählen. Dabei müssen Sie darauf achten, dass die ausgewählten Repräsentanten nicht zu den Geräten gehören, auf denen Sie Abbilder bereitstellen. Wenn Sie versuchen, Abbilder von Multicast-Domänenrepräsentanten in einem Subnetz zu erstellen, schlägt diese Abbilderstellung fehl und die Geräte weisen anschließend einen Zustand auf, in dem sie nicht mehr funktionsfähig sind.

Angeben, welche Geräte als Multicast-Domänenrepräsentanten fungieren

Sie können manuell festlegen, welche Geräte als Multicast-Domänenrepräsentanten verwendet werden sollen, indem Sie Geräte zur Gruppe **Konfiguration > Multicast-Domänenrepräsentanten** in der Netzwerkansicht hinzufügen.

Drosseln der Multicast-Bandbreite

Sie können die von Multicasts verwendete Bandbreite durch Änderungen der Optionen im Assistenten für die Betriebssystembereitstellung drosseln. Wählen Sie im Skript "Abbild bereitstellen" die folgenden Optionen aus:

1. Wählen Sie auf der Seite **Methoden und Anmeldeinformationen** die Option **Multicastdownload** aus.
2. Wählen Sie auf der Seite **Multicast-Erkennung** die Option **Erweiterte Multicastoptionen konfigurieren**.
3. Ändern Sie auf der Seite **Erweiterte Optionen** die Optionen so, wie dies zur Reduzierung des Netzwerkverkehrs erforderlich ist.

WARNUNG: Wenn die Multicasting-Umgebung nicht richtig konfiguriert ist und der Targeted Multicast fehlschlägt, kann es sein, dass sich keines der Zielgeräte starten lässt, sofern nicht die oben beschriebenen Richtlinien befolgt werden.

Wenn der Targeted Multicast bei Verteilungsaufträgen fehlschlägt, liegt dies u. U. daran, dass die MTU-Größe (Maximum Transmission Unit) in Ihrem Netzwerk Pakete fragmentiert.

Verwandte Themen

"Festlegen der maximalen Paketgröße für einen Targeted Multicast mit der Betriebssystembereitstellung (OSD)" auf Seite 395

"Erstellen einer Imaging-Bootdiskette" auf Seite 426

Festlegen der maximalen Paketgröße für einen Targeted Multicast mit der Betriebssystembereitstellung (OSD)

Wenn der Targeted Multicast bei Verteilungsaufträgen fehlschlägt, liegt dies u. U. daran, dass die MTU-Größe (Maximum Transmission Unit) in Ihrem Netzwerk Pakete fragmentiert. Die MTU in Ihrem Netzwerk bestimmt die maximale Paketgröße. Führen Sie die nachfolgend beschriebenen Schritte aus, um die von Multicast verwendete MTU anzupassen.

So setzen Sie die maximale Paketgröße für ein Targeted Multicast-Skript auf 512 Byte

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie mit der rechten Maustaste auf das Skript, und klicken Sie auf **Erweiterte Bearbeitung**.
3. Fügen Sie die folgende Zeile am End des Multicast-Abschnitts zum Skript hinzu.

   MAX_PACKET_SIZE=512

   Diese Zeichenfolge setzt die maximale Paketgröße für den Targeted Multicast auf 512 Byte. Die maximale Paketgröße kann auf einen Wert zwischen 256 und 1464 Byte gesetzt werden. Eine Einstellung oberhalb dieses Bereichs oder keine Einstellung erzwingt die Standardeinstellung 1464. Eine Einstellung unterhalb dieses Bereichs wird standardmäßig in 256 Byte konvertiert.
4. Speichern und schließen Sie das Skript.

WARNUNG: Die Einstellung MAX_PACKET_SIZE muss mindestens 28 Byte kleiner sein als die Maximum Transmission Unit (MTU) für das Netzwerk, in dem das Paket verteilt wird. Dieser Wert wird durch Addieren der Größe des mit jedem Datenpaket gesendeten IP-Headers (20 Byte) und des UDP-Headers (8 Byte) ermittelt. Wenn die maximale Paketgröße auf einen Wert eingestellt wird, der diesen Grenzwert überschreitet, schlägt die Verteilung fehl.

Anzeigen von Abbildstatusberichten

Ein abgebildetes Gerät sendet Statusupdates an den Coreserver. Sie können den Status im Fenster "Benutzerdefinierter Auftrag" oder in einem Bericht überwachen.

Wenn die Betriebssystembereitstellung Abbilderstellungsbefehle an Geräte sendet, werden die Befehle im Fenster "Benutzerdefinierter Auftrag" angezeigt. Geräte, von denen ein Abbild erstellt wird, senden Statusaktualisierungen für jeden gesendeten Skriptbefehl. Falls die Abbildbereitstellung misslingt, wird der Befehl, dessen Ausführung misslungen ist, angezeigt.

Allgemeine Gründe für das Fehlschlagen der Abbilderstellung:

- Beschädigte Partition.
- Probleme, die vom Abbilderstellungstool nicht bewältigt werden können.
- Die automatische Netzwerkadapter-Erkennung findet keinen Netzwerkadapter.
- Der von Ihnen angegebene, nicht auffindbare Netzwerkadapter ist nicht kompatibel. Wenn der angegebene Netzwerkadaptertreiber nicht geladen wird, hält das Gerät bei der DOS-Eingabeaufforderung an. Sie müssen es dann manuell neu starten.

Die Betriebssystembereitstellung erstellt einen Statusbericht für jeden Auftrag und zeigt darin, ob der Auftrag auf den Zielgeräten erfolgreich ausgeführt wurde oder nicht.

Erstellen von Skripten für die Abbilderstellung

Die Betriebssystembereitstellungsfunktion von LANDesk stellt die Extras zur Betriebssystembereitstellung und Profilmigration zur Verfügung, mit denen Sie sowohl Skripte für die Abbilderstellung (Abbilderfassung und -bereitstellung) als auch für die Profilmigration erstellen können.

Mit dem Betriebssystembereitstellungstool können Sie Skripte für die Ausführung folgender Tasks erstellen:

- **Abbild erfassen:** Erstellt ein Skript, das ein Betriebssystemabbild von einem Gerät erstellt und speichert. Abbilder können mithilfe des integrierten LANDesk Abbilderstellungstools oder mit einem Tool eines anderen Herstellers, z. B. Ghost oder PowerQuest, aufgezeichnet werden.
- **Profil erfassen:** Erstellt ein Skript, das die einem Gerät eigenen Benutzereinstellungen, Anwendungs- und Desktop-Einstellungen sowie Dateien erfasst. Mit dieser Option können Sie auch auf das Dialogfeld "Sammlungsmanager" zugreifen, um ein benutzerinitiiertes Profilmigrationspaket zu erstellen, das lokal auf einzelnen Geräten ausgeführt werden kann.
- **Abbild bereitstellen:** Erstellt ein Skript, das ein zuvor erstelltes Betriebssystemabbild auf Zielgeräte bereitstellt.
- **Profil wiederherstellen:** Erstellt ein Skript, das zuvor erfasste Profildaten auf Zielgeräten wiederherstellt (Benutzereinstellungen, Anwendungs- und Desktop-Einstellungen sowie Dateien).
- **Generische DOS-Tasks:** Erstellt ein Skript, das auf Geräten DOS-Befehle ausführt (einschließlich Anwendungsstart).

Nachdem Sie ein Skript erstellt haben, können Sie über **Geplante Tasks** die Ausführung des Skripts auf Geräten planen.

HINWEIS: Erstellen von benutzerinitiierten Profilmigrationspaketen
Im Assistenten für Tasks zur Betriebssystembereitstellung/Migration können Sie auch auf das Dialogfeld "Sammlungsmanager" zugreifen. In diesem Dialogfeld können Sie ein benutzerinitiiertes Profilmigrationspaket (eine selbstextrahierende ausführbare Datei) erstellen, das für die benutzerinitiierte

Profilmigration auf Geräten bereitgestellt und ausgeführt werden kann. Weitere Informationen finden Sie unter "Migrieren von Benutzerprofilen" auf Seite 409.

Wenn Sie ein Abbild auf PXE-kompatiblen Geräten bereitstellen, können Sie Skripte für die Abbildbereitstellung in das PXE-DOS-Startmenü einfügen. Dieses Menü ist DOS-basiert und wird beim PXE-Start auf dem Gerät angezeigt.

Administratoren (Benutzer mit LANDesk-Administratorrechten) können Skripte in Benutzeruntergruppen in der Gruppe **Benutzerskripte** kopieren.

Hinweise zur Verwendung von Skripten

- Skriptnamen müssen den Windows-Dateinamenskonventionen entsprechen. Der Assistent verwendet den eingegebenen Skriptnamen als Dateinamen. Wenn Sie Zeichen verwenden, die in Windows-Dateinamen nicht zulässig sind, wird eine entsprechende Meldung ausgegeben.
- Alle Skripte werden auf dem Coreserver im Verzeichnis \\<Core>\LDMain\Scripts gespeichert. Wenn Sie mehrere Konsolen verwenden, werden die Skripte im Fenster "Skripte verwalten" der jeweiligen Konsole angezeigt.
- Auf den Assistentenseiten werden die Einstellungen des zuletzt erstellten Skripts wiederhergestellt. Wenn Sie den Skripttyp von einem Abbilderstellungstask in einen Profilmigrationstask oder einem DOS-Task ändern, löscht der Assistent die gespeicherten Einstellungen.
- Aufgrund von Änderungen in Bezug auf die Art und Weise, wie die Berechtigungen des Administratorbenutzerkontos in Windows Vista und insbesondere in Windows 7 gehandhabt werden, werden Sie unter Umständen feststellen, dass von Ihnen erstellte Masterabbilder, die diese Windows-Versionen einschließen, nicht erfolgreich bereitgestellt werden können. Wir empfehlen Ihnen, die Website der LANDesk Support Community unter community.landesk.com zu besuchen und sich die Dokumente zu den bekanntesten Methoden anzusehen, in denen Szenarien für Masterabbilder und empfohlene Verfahren zur Erstellung und Bereitstellung von Abbildern beschrieben sind.

Informationen über die Skripte "Generische DOS-Tasks"

- DOS-Skripte starten die ausgewählten Zielgeräte neu und führen die angegebenen Befehle aus. Diese Remotebefehle werden zeilenweise gesendet.
- DOS-Skripte werden von der virtuellen Startpartition ausgeführt und durchlaufen denselben Netzwerkerkennungsprozess wie normale Betriebssystemverteilungen.
- Mit der Option "Diesen Task abbrechen, wenn ein Befehl fehlschlägt" wird die Ausführung angehalten, falls einer der Befehle eine DOS-Fehlerebene ungleich Null zurückgibt. Sie können den Status des DOS-Tasks im Fenster "Benutzerdefinierter Auftrag" oder in einem Bericht überprüfen.

Erstellen eines Skripts für die Profilerfassung

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** mit der rechten Maustaste auf **Alle OSD-Skripte** und wählen Sie den PE-Typ aus, den Sie verwenden möchten (beispielsweise Neue Windows PE-Konfiguration).
3. Wählen Sie **Profil erfassen** und klicken Sie anschließend auf **OK**.
4. Der daraufhin angezeigte Assistent führt Sie durch die Skripterstellung. Füllen Sie alle Felder aus. Klicken Sie hierzu nacheinander auf alle Elemente, um sämtliche Felder anzuzeigen.

5. Wenn Sie Hilfe zu einem Feld benötigen, klicken Sie auf **Hilfe**.
6. Wenn das Skript vollständig ist, klicken Sie auf **Speichern**.

Wenn der Vorgang abgeschlossen ist, wird das Skript in der Gruppe **Alle OSD-Skripte** im Fenster **Betriebssystembereitstellung** angezeigt.

Erstellen eines Skripts für die Abbildbereitstellung

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** mit der rechten Maustaste auf **Alle OSD-Skripte** und wählen Sie den PE-Typ aus, den Sie verwenden möchten (beispielsweise Neue Windows PE-Konfiguration).
3. Wählen Sie **Abbild bereitstellen** und klicken Sie anschließend auf **OK**.
4. Der daraufhin angezeigte Assistent führt Sie durch die Skripterstellung. Füllen Sie alle Felder aus. Klicken Sie hierzu nacheinander auf alle Elemente, um sämtliche Felder anzuzeigen.
5. Wenn Sie Hilfe zu einem Feld benötigen, klicken Sie auf **Hilfe**.
6. Wenn das Skript vollständig ist, klicken Sie auf **Speichern**.

Wenn der Vorgang abgeschlossen ist, wird das Skript in der Gruppe **Alle OSD-Skripte** im Fenster **Betriebssystembereitstellung** angezeigt.

Ändern von Skripten für die Abbilderstellung

Sie können Ihre Skripte jederzeit bearbeiten, entweder indem Sie das Konfigurationsdialogfeld erneut öffnen und Änderungen vornehmen, oder indem Sie das Skript direkt in der .ini-Datei bearbeiten und alle bestehenden Sysprep-Einstellungen in der zugehörigen .inf-Datei bearbeiten.

HINWEIS: Bei DOS-Skripten dürfen ausschließlich Änderungen zwischen den Zeilen REMPINGx=DOS und REMEXECx=reboot.com vorgenommen werden. Die anderen Zeilen im Skript sind für die virtuellen Startpartitionsdateien und den Startprozess verantwortlich.

So ändern Sie ein Skript mithilfe des Konfigurationsassistenten

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie mit der rechten Maustaste auf das Skript, und klicken Sie im Kontextmenü auf **Bearbeiten** (oder doppelklicken Sie auf das Skript).
3. Führen Sie den Assistenten Schritt für Schritt aus und nehmen Sie die gewünschten Änderungen vor.

So ändern Sie ein Skript durch Bearbeitung der .ini-Datei

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie mit der rechten Maustaste auf das Skript, und klicken Sie auf **Erweiterte Bearbeitung**. Die .ini-Datei des Skripts wird im Editor geöffnet. Wenn es für dieses Skript Sysprep-Einstellungen gibt, wird die sysprep.inf-Datei ebenfalls im Editor geöffnet.
3. Nehmen Sie die gewünschten Änderungen an einer der Dateien oder an beiden Dateien vor.
4. Speichern Sie die Dateien.

HINWEIS: INI-Dateien werden im Verzeichnis \\<core>\LDMain\Scripts gespeichert. INF-Dateien werden im

Verzeichnis \\<core>\LDMain\LANDesk\Files gespeichert.

Hardwareunabhängige Abbilderstellung – Übersicht

Bei der Bereitstellung von Abbildern für verwaltete Geräte stellt die Verwaltung der vielen verschiedenen Abbilder, die auf unterschiedlichen Hardwarekonfigurationen aufbauen, eine Herausforderung dar. Neue Hardware erfordert neue Treiber und für vorhandene Hardware gibt es unter Umständen Treiberupdates, die Sie bereitstellen möchten. Statt Dutzende oder Hunderte verschiedener Einzelabbilder für verschiedene Hardwarekonfigurationen zu verwalten, können Sie die hardwareunabhängige Abbilderstellung (HII, hardware-independent imaging) verwenden, um ein Basisabbild für verschiedene Geräte bereitzustellen und dann automatisch die Treiber hinzufügen, die für jeden einzelnen Typ von Hardware erforderlich sind.

Die hardwareunabhängige Abbilderstellung trägt zur Lösung häufig auftretender Probleme bei der Abbilderstellung für verwaltete Geräte bei. So müssen beispielsweise die .dll-Dateien der Hardwareabstraktionsschicht (HAL) ganz korrekt gewählt werden, sonst startet das Gerät nach der Abbilderstellung unter Umständen mit einem schwarzen Bildschirm. Betriebssysteme können Massenspeichergeräte in der Regel nicht korrekt erkennen, daher ist es von entscheidender Bedeutung, bei der Abbilderstellung die richtiger Treiber zu haben. Darüber hinaus haben Hersteller häufig hardwarespezifische Plug-and-Play-Gerätetreiber oder sie bauen Treiberabhängigkeiten in ihre Anwendungen ein, so dass unter Umständen neue Probleme entstehen, wenn ein Gerät beim Imaging mit den falschen Treibern bestückt wird. Mit dem hardwareunabhängigen Abbilderstellungstool der LANDesk Management Suite können Sie diese Art von Problemen vermeiden und Sie haben außerdem eine bessere Kontrolle darüber, welche Treiber in Ihren verwalteten Geräten verwendet werden.

Sie können das Extra für die hardwareunabhängige Abbilderstellung in Verbindung mit Abbildern jedes beliebigen Abbilderstellungstools verwenden. Sie können die Abbilder mit dem von Ihnen bevorzugten Tool definieren und dann Abbilderstellungsskripte in Management Suite erstellen, die das Extra zur hardwareunabhängigen Abbilderstellung einbeziehen. Wenn Sie bereits mit einem anderen Tool Abbilder erstellt haben, können Sie diese wiederverwenden, statt von Grund auf neue Skripte zu erstellen.

Der HII-Prozess zur hardwareunabhängigen Abbilderstellung wird nachstehend vereinfacht beschrieben. Einzelheiten zu den spezifischen Schritten, die Sie befolgen müssen, sowie Überlegungen zu verschiedenen Arten von Abbildern werden in den folgenden Abschnitten beschrieben.

1. Wenn Sie ein mit HII erstelltes Abbild bereitstellen, startet das Abbilderstellungsskript das Gerät in die Windows-Prebootumgebung. In der Prebootumgebung wählt das HII-Extra die entsprechende HAL .dll-Datei aus und lädt diese.
2. Das Betriebssystem wird auf dem Gerät installiert, aber bevor das Betriebssystem startet, bestimmt das HII-Abbilderstellungsskript, welche Treiber für das Gerät erforderlich sind, und kopiert die Treiberdateien auf die Festplatte des Geräts.
3. Die Treiber werden zur Registrierung des Geräts hinzugefügt, so dass das Windows-Installationsprogramm beim Starten des Betriebssystems die neuen Treiber erkennt, diese installiert und das Gerät mit den Treibern konfiguriert.
4. Windows startet dann neu mit den geladenen Treibern und der LANDesk Agent wird installiert.

HINWEIS: Aufgrund von Änderungen in Bezug auf die Art und Weise, wie die Berechtigungen des Administratorbenutzerkontos in Windows Vista und insbesondere in Windows 7 gehandhabt werden, werden Sie unter Umständen feststellen, dass von Ihnen erstellte Masterabbilder, die diese Windows-

Versionen einschließen, nicht erfolgreich bereitgestellt werden können. Wir empfehlen Ihnen, die Website der LANDesk Support Community unter community.landesk.com zu besuchen und sich die Dokumente zu den bekanntesten Methoden anzusehen, in denen Szenarien für Masterabbilder und empfohlene Verfahren zur Erstellung und Bereitstellung von Abbildern beschrieben sind.

Einrichten der hardwareunabhängigen Abbilderstellung

Um die hardwareunabhängige Abbilderstellung mit Betriebssystembereitstellungsskripten oder Versorgungsvorlagen zu implementieren, erstellen Sie ein Repository von Treibern, die dann für das Abbilderstellungstool zur Verfügung stehen. Diese Treiber werden auf der Hardware verwendet, die Sie abbilden, und umfassen Treiber für Audio-, Video-, Netzwerkgeräte, Massenspeichergeräte und andere Gerätetypen.

Speichern Sie die Treiber an einem Speicherort auf einem bevorzugten Server und stellen Sie sicher, dass auf diesen Pfad sowohl über UNC als auch über HTTP zugegriffen werden kann.

Wenn das Tool zur hardwareunabhängigen Abbilderstellung ausgeführt wird, erkennt es den Gerätehersteller und das Modell, lädt dann die zugehörigen Treiber herunter und installiert sie während des Abbilderstellungsprozesses auf dem Gerät.

Im folgenden Abschnitt wird beschrieben, wie ein Repository erstellt wird. Darüber hinaus erhält der Abschnitt Hinweise dazu, wie die hardwareunabhängige Abbilderstellung in Skripte für die Betriebssystembereitstellung und in Versorgungsvorlagen eingebunden werden kann.

Erstellen eines Treiberrepositorys

Bei der Planung und Definition der Abbilder, die Sie für verwaltete Geräte verwenden möchten, entscheiden Sie, welche Treiber Sie einsetzen möchten. Damit Sie diese Treiber für die hardwareunabhängige Abbilderstellung verwenden können, erstellen Sie ein Treiberrepository, das an einem einzigen Ort gespeichert wird (standardmäßig auf dem Management Suite Coreserver). Die Treiber stehen dann für Bereitstellungs- oder Versorgungsskripte bereit, die Sie ausführen möchten.

Zur Erstellung eines Repositorys müssen die Treiberdateien in einem Ordner gespeichert werden. Für jeden Treiber muss eine .inf-Datei enthalten sein. Das HII-Extra scannt den Ordner und erstellt eine drivers.db3-Datei, die dazu verwendet wird, Gerätehardware mit den entsprechenden Treibern abzugleichen.

So erstellen Sie ein Treiberrepository

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Treiberbibliothek verwalten**.
3. Vergewissern Sie sich, dass der Speicherort des Repositorys korrekt ist. Wenn Treiberdateien an einem anderen Speicherort abgelegt sind, klicken Sie auf **Durchsuchen** und wählen Sie Ihren Repositoryordner aus.
4. Vergewissern Sie sich, dass die URL korrekt ist, die auf den Speicherort des Repositorys verweist.

5. Klicken Sie auf **Speichern**.

   Das HII-Extra scannt den Repositoryordner und erstellt eine Liste von Treibern. Nach Abschluss dieses Vorgangs wird in einer Erfolgsmeldung eine Dateianzahl für das Repository (d. h. wie viele Dateien gefunden wurden) angezeigt sowie die Anzahl der verarbeiteten Treiber (d. h. wie viele einzelne Treiber gefunden wurden).
6. Jedes Mal, wenn Sie Treiberdateien zum Repositoryordner hinzufügen, müssen Sie die Schritte 1 bis 5 wiederholen, um die drivers.db3-Datei mit den neuen Daten zu aktualisieren.

Verwendung der hardwareunabhängige Abbilderstellung (HII) mit Skripten für die Betriebssystembereitstellung

Sie können die hardwareunabhängige Abbilderstellung in Skripte für die Betriebssystembereitstellung für Windows-Geräte einbinden, wenn das Skript die folgenden Bedingungen erfüllt:

- Es muss auf der Windows PE-Bootumgebung basieren.
- Es muss Windows Sysprep zur Konfiguration des Betriebssystemabbilds verwenden.

Um die hardwareunabhängige Abbilderstellung zu integrieren, müssen Sie im Skriptassistenten die HII-Option auswählen, damit das HII-Extra im Anschluss an die Betriebssysteminstallation ausgeführt wird. Das HII-Extra wählt auf der Basis von Zeichenfolgen im BIOS des Geräts automatisch den Hersteller und das Modell des Geräts aus, für das Sie ein Abbild erstellen.

So schließen Sie die hardwareunabhängige Abbilderstellung (HII) in Skripte für die Betriebssystembereitstellung ein

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie unter **OSD-Skripte** ein Skript aus. Klicken Sie mit der rechten Maustaste auf das Skript und wählen Sie **Bearbeiten** aus. Sie können aber auch ein neues Skript erstellen, indem Sie mit der rechten Maustaste auf **Alle OSD-Skripte** klicken und **Neue Windows PE-Konfiguration** auswählen.
3. Klicken Sie auf **Methoden und Anmeldeinformationen**. Aktivieren Sie die Kontrollkästchen **Abbild verwendet SysPrep** und **Abbild wird von SysPrep verarbeitet**.
4. Klicken Sie auf **SysPrep-Optionen > Hardwareunabhängige Abbildoptionen**.
5. Um festzulegen, dass ausschließlich UNC für den Zugriff auf das HII-Repository verwendet wird, aktivieren Sie das Kontrollkästchen **UNC zum Kopieren von Treiberdateien verwenden**.
6. Definieren Sie alle anderen gewünschten Skriptoptionen und klicken Sie auf **Speichern**, um das Skript zu speichern.

Verwendung der hardwareunabhängige Abbilderstellung (HII) mit Versorgungsvorlagen

Sie können die hardwareunabhängige Abbilderstellung in Versorgungsvorlagen für Windows-Geräte einbinden, wenn die Vorlage die folgenden Bedingungen erfüllt:

- Es muss auf der Windows PE-Bootumgebung basieren.
- Es muss Windows Sysprep zur Konfiguration des Betriebssystemabbilds verwenden.

Um die hardwareunabhängige Abbilderstellung (HII) einzubinden, müssen Sie eine HII-Option im Abschnitt **Nach der Installation des Betriebssystems** der Vorlage hinzufügen, damit das HII-Extra nach der Installation des Betriebssystems ausgeführt wird. Das HII-Extra wählt anhand der Zeichenfolgen im Geräte-BIOS automatisch den Hersteller und das Modell des Geräts aus, das Sie versorgen.

So schließen Sie die hardwareunabhängige Abbilderstellung (HII) in eine Versorgungsvorlage ein

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie unter **Versorgungsvorlagen** ein Windows-basierte Vorlage aus. Klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Bearbeiten** aus. Oder, falls Sie eine neue Vorlage erstellen möchten, klicken Sie auf die Schaltfläche **Neue Versorgungsvorlage**, benennen die Vorlage, wählen die Windows PE-Bootumgebung und anschließend das Zielbetriebssystem aus.
3. Klicken Sie auf **Aktionsliste** und dann auf den Abschnitt **Nach der Installation des Betriebssystems**.
4. Klicken Sie auf **Hinzufügen**. Geben Sie einen Namen und eine Beschreibung für die Aktion ein (z. B. HII) und wählen Sie dann in der Liste **Typ** den Eintrag **Hardwareunabhängige Abbilderstellung** aus. Klicken Sie auf **OK**.
5. Um festzulegen, dass ausschließlich UNC für den Zugriff auf das HII-Repository verwendet wird, aktivieren Sie das Kontrollkästchen **UNC zum Kopieren von Treiberdateien verwenden**.
6. Klicken Sie auf **Übernehmen**, um die HII-Aktion mit der Vorlage zu speichern, und fügen Sie danach bei Bedarf andere Aktionen zur Vorlage hinzu. Sie sollten unbedingt *nach* der HII-Aktion eine Aktion vom Typ **Neu starten** in den Abschnitt **Nach der Installation des Betriebssystems** einschließen.
7. Nehmen Sie eventuell erforderliche Änderungen für andere Variablen, eingeschlossene Vorlagen oder andere Einstellungen für die Vorlage vor und klicken Sie auf **OK**, wenn Sie fertig sind.

Übersicht über die Profilmigration

Mit der Profilmigration können Sie benutzerdefinierte Benutzerprofile, Desktops, Einstellungen für Anwendungen, Netzwerkverbindungen, Drucker, Dateien und Ordner bewahren, wenn Sie Upgrade- oder Migrationsprojekte durchführen. Die Profilmigration unterstützt Direktmigrationen einzelner Geräte sowie umfangreiche Remotemigrationen mehrerer Geräte über das Netzwerk.

Für Migrationstasks kommt das Extra "Benutzermigrations-Assistent" zum Einsatz, das auf allen verwalteten Geräte ausgeführt wird, um Profile zu erfassen und diese auf einem neuen Betriebssystem wiederherzustellen. Wenn Sie einen Skript für die Betriebssystembereitstellung planen, wird der Benutzermigrations-Assistent auf dem verwalteten Gerät installiert, nachdem der Task "Profil erfassen" bzw. "Profil wiederherstellen" zum ersten Mal auf dem Gerät ausgeführt wurde. Sie können den Benutzermigrations-Assistenten nach seiner Installation auch als eigenständiges Extra auf verwalteten Geräten ausführen.

Die Profilmigration ist ein zweigeteilter Prozess:

1. *Erfassen* des eindeutigen Profils eines Quellgeräts, bestehend aus Benutzerkonten, Desktop (PC)- und Anwendungseinstellungen, Netzwerkeinstellungen, Drucker sowie Datendateien und Ordnern.
2. *Wiederherstellen* des Profils auf einem Zielgerät.

Funktionsprinzip der Profilmigration

Mit der Profilmigration können Sie separate Skripte für die Erfassung und die Wiederherstellung erstellen. Jedes dieser Skripte kann anschließend remote auf einem oder mehreren Zielgeräten im Netzwerk ausgeführt werden. Den eigentlichen Prozess der Erfassung und Wiederherstellung von Profilen übernimmt der Benutzermigrations-Assistent, eine ausführbare Datei, die bei der Skriptausführung im Hintergrund installiert wird.

Elemente, die erfasst werden, sind in der Befehlsdateiquelle des Benutzermigrations-Assistenten, einer XML-Datei, aufgelistet. Jedes Element in der Datei kann ein- und ausgeschaltet werden, indem es auf True (Wahr) oder False (Falsch) gesetzt wird. Die Einstellung `<mouse>true</mouse>` bedeutet beispielsweise, dass die Mauseinstellung des Benutzers erfasst wird. Ein Beispiel für eine Befehlsdatei finden Sie im Order <Coreserver>\ldlogon\uma\commandxml.

Voraussetzungen

Eine Profilmigration ist nur möglich, wenn Geräte folgende Voraussetzungen erfüllen:

- Geräte müssen in die Coredatenbank gescannt werden.
- Auf den Geräten müssen der Standard LANDesk Agent, der den Inventarscanner und Local Scheduler umfasst, und der Softwareverteilungsagent installiert sein. Die Profilmigration verwendet den Softwareverteilungsagenten, um Dateien zu verteilen.

Migrationspfade

Die Profilmigration unterstützt die Migration zwischen folgenden Versionen von Windows-Betriebssystemen:

- Windows 2000 Professional
- Windows XP Home
- Windows XP Tablet PC Edition 2005
- Windows XP Professional
- Windows Vista Home Basic 32-Bit
- Windows Vista Home Premium 32-Bit
- Windows Vista Business 32-Bit
- Windows Vista Ultimate 32-Bit
- Windows Vista Home Basic 64-Bit
- Windows Vista Home Premium 64-Bit
- Windows Vista Business 64-Bit
- Windows Vista Ultimate 64-Bit
- Windows 7 Home Premium 32-Bit
- Windows 7 Professional 32-Bit
- Windows 7 Ultimate 32-Bit
- Windows 7 Home Premium 64-Bit
- Windows 7 Professional 64-Bit
- Windows 7 Ultimate 64-Bit

Arbeitsumgebungen können von einem 32-Bit-Betriebssystem auf ein 64-Bit-Betriebssystem migriert werden, aber nicht umgekehrt. Die Quell- und Zielgeräte müssen dieselbe Sprachversion von Windows verwenden.

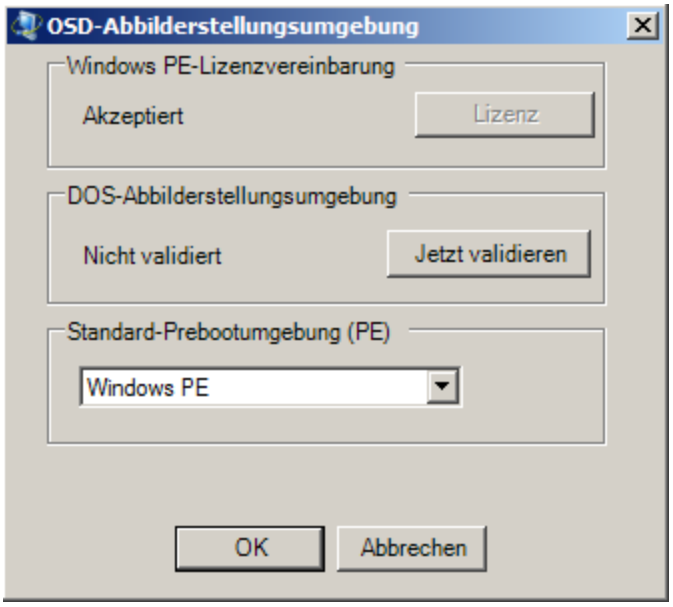
Eine ausführliche Liste zulässiger Migrationsszenarien finden Sie im Dokument "Using profile migration in LANDesk Management Suite 9", das Sie bei der LANDesk Supportcommunity unter community.landesk.com herunterladen können.

Erstellen von Profilmigrationsskripten

Den Assistenten für die Betriebssystembereitstellung verwenden Sie zur Erstellung von Skripten zur Erfassung und Wiederherstellung von Geräteprofilen. Zur Erstellung von Profilmigrationsskripten können Sie die DOS- oder die Windows PE-Umgebung verwenden.

Voraussetzungen

Bevor Sie Profilmigrationsskripte erstellen können, müssen Sie die Lizenzen Ihrer Betriebssystem-Prebootumgebungen (PE, Preboot Environment) für DOS PE und Windows PE validieren Hierzu klicken Sie auf die Schaltfläche **Lizenzen validieren** in der Symbolleiste der Betriebssystembereitstellung.



Bei der DOS PE-Umgebung erfordert die Lizenzverifizierung eine Windows NT 4 Server- und eine Windows 98-CD.

Bei der Windows PE-Umgebung müssen Sie die Lizenz für die Windows PE-Umgebung akzeptieren, die mit diesem Produkt installiert wird.

Speichern von Profildaten für mehrere Geräte (und mehrere Benutzer)

Profildaten werden in System Migration Assistant (.sma)-Dateien in einer Verzeichnisstruktur gespeichert, die sich unter dem angegebenen UNC-Pfad befindet. Wenn Sie ein Profilerfassungsskript auf mehreren Geräten ausführen, werden die Profildaten des jeweiligen Geräts in separaten Verzeichnissen gespeichert, die nach ihren eindeutigen Windows-Computernamen benannt werden.

Genauso verhält es sich auch mit Benutzern: Wenn mehrere Benutzer auf demselben Quellgerät erkannt und aufgezeichnet werden, werden die Profildaten der einzelnen Benutzer in separaten Unterverzeichnissen des Geräteverzeichnisses gespeichert, die entsprechend dem Benutzeranmeldenamen benannt werden. Das heißt, jedes migrierte Gerät besitzt ein eigenes Profilspeicherverzeichnis und ein Unterverzeichnis für jedes erfasste Benutzerkonto auf diesem Gerät.

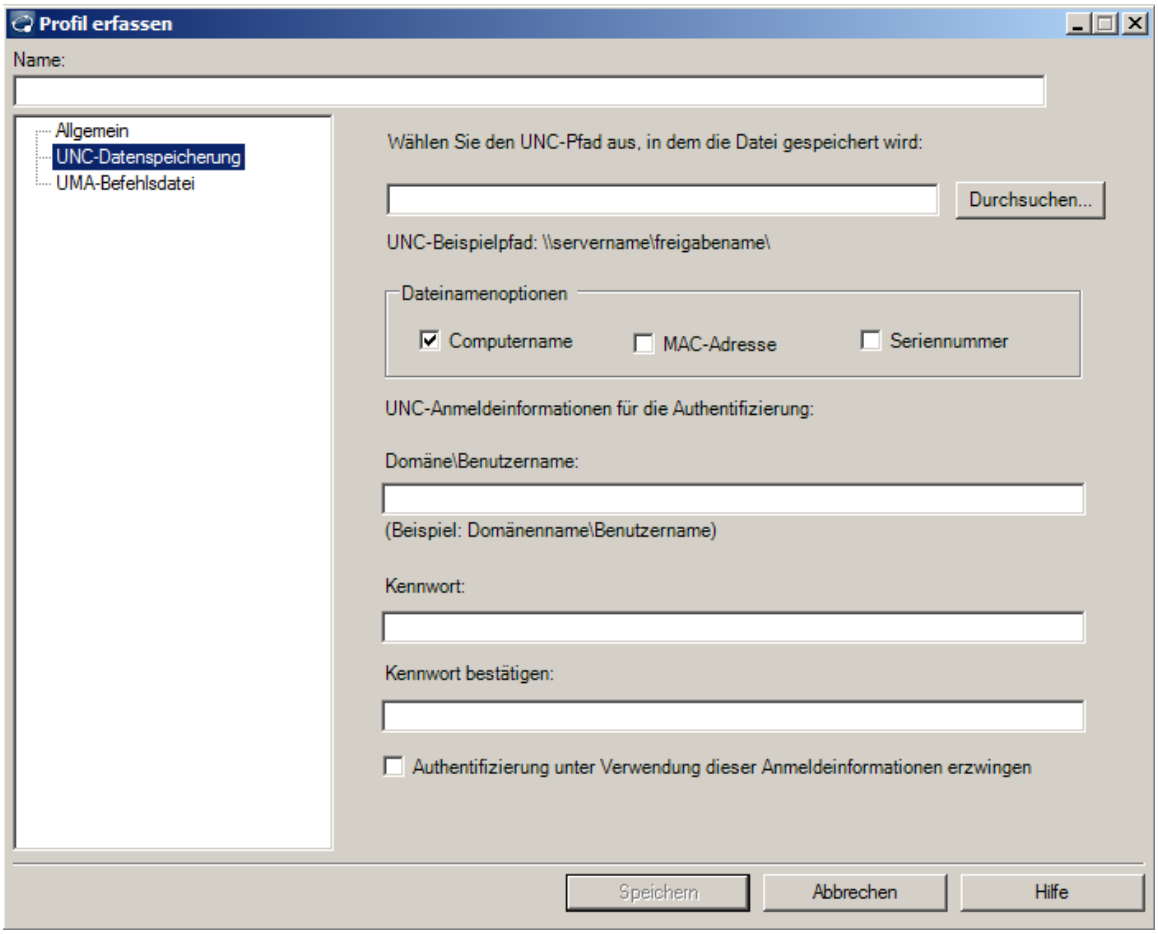
Protokolldatei der Profilmigration

Die Profilmigration erstellt eine Protokolldatei für jedes von Ihnen ausgeführte Skript. Protokolldateien werden auf dem Coreserver im Ordner <Coreserver>\ldlog gespeichert. Protokolldateien werden wie folgt benannt: `CJ-OSD-Skriptname-Datum-Uhrzeit.log`

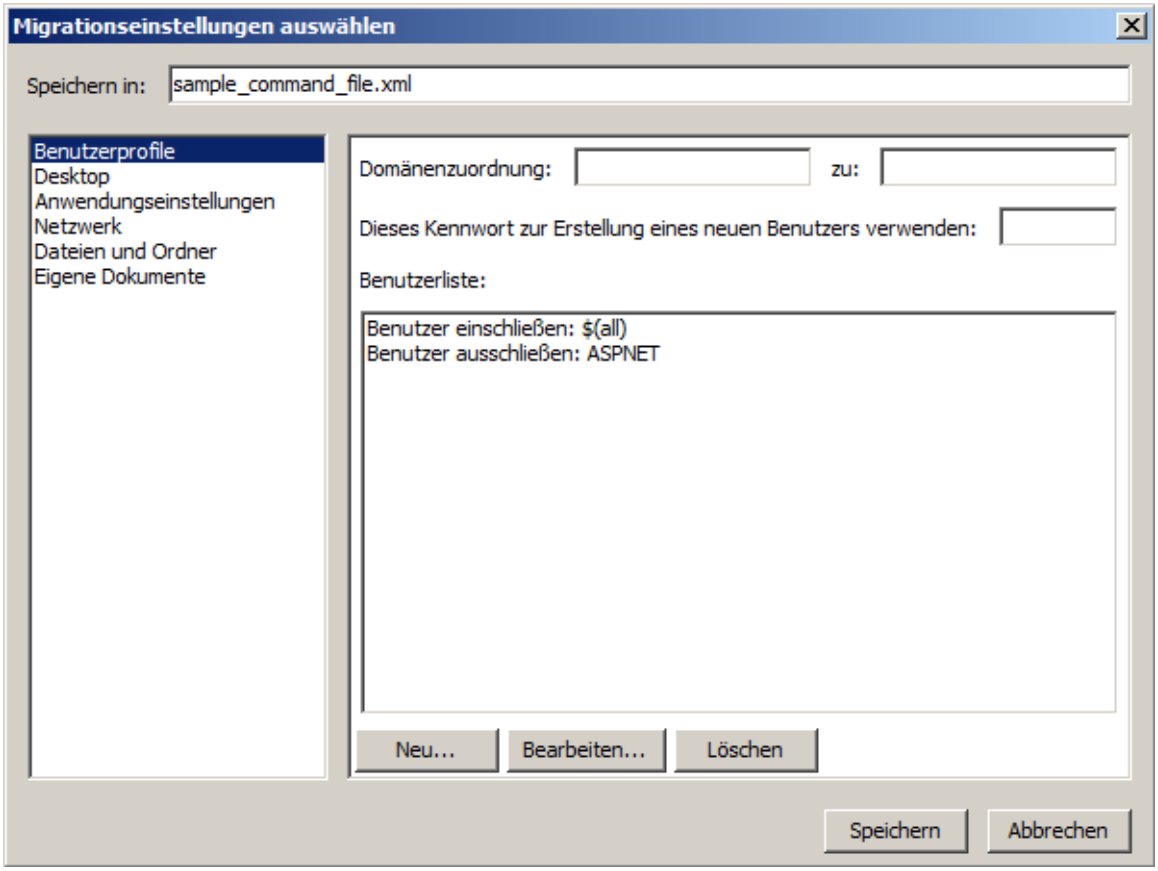
Erstellen eines Profilerfassungsskripts

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** auf **Eigene OSD-Skripte** oder **Alle OSD-Skripte**.
3. Klicken Sie auf die Symbolleisten-Schaltfläche für die PE-Umgebung, die Sie verwenden möchten (entweder **Neue DOS PE-Konfiguration** oder **Neue Windows PE-Konfiguration**).
4. Wählen Sie **Profil erfassen** und klicken Sie anschließend auf **OK**.
5. Geben Sie auf der Seite **Allgemein** einen Namen und eine Beschreibung für das Skript ein. Wenn Sie möchten, dass die Profilerfassung auch dann fortgesetzt wird, wenn Fehler auftreten, markieren Sie das Kontrollkästchen **Mit Dateiaufzeichnungsfehlern fortfahren**. (Wenn Sie diese Option aktivieren, werden Dateifehler in der Protokolldatei aufgezeichnet.)
6. Geben Sie auf der Seite **UNC-Speicher** einen UNC-Pfad und -Anmeldeinformationen für die Authentifizierung für das Verzeichnis ein, in dem die Profildaten gespeichert werden sollen.
    - Geben Sie ein Dateinamensmuster für die Speicherung der Profildaten an. Verwenden Sie eine beliebige Kombination aus Computername, MAC-Adresse und Seriennummer für die Erstellung eines Dateinamens für das Profil. (Wenn Sie beispielsweise **Seriennummer** wählen und die Seriennummer des Geräts lautet 12345678, dann wird der Profilname als "12345678.sma" gespeichert.)
    - Markieren Sie das Kontrollkästchen **Authentifizierung erzwingen**, wenn Sie auf Geräten, für die eine Profilmigration geplant ist, eine Authentifizierung erzwingen wollen, falls die

Anmeldeinformationen des aktuell angemeldeten Benutzer nicht ausreichen.



7. Geben Sie auf der Seite **UMA-Befehlsdatei** den Namen und den Speicherort der Befehlsdatei ein, die für die Profilmigration verwendet wird. Klicken Sie auf **Bearbeiten**, um eine neue Befehlsdatei zu erstellen oder eine vorhandene Befehlsdatei zu bearbeiten.
    - Wählen Sie im Dialogfeld **Migrationseinstellungen** eine vorhandene Befehlsdatei aus und klicken Sie auf **Bearbeiten** oder Klicken Sie auf **Neu**, um eine neue Befehlsdatei zu erstellen.
    - Klicken Sie auf **Benutzerprofile** und fügen Sie die Benutzerprofile hinzu, die Sie bei der Migration erfassen möchten.
    - Klicken Sie auf **Desktop** und markieren Sie das Kontrollkästchen aller Elemente, die bei der Migration erfasst werden sollen.
    - Klicken Sie auf **Anwendungseinstellungen** und markieren Sie das Kontrollkästchen aller Anwendungen, die bei der Migration erfasst werden sollen.
    - Klicken Sie auf **Netzwerk** und markieren Sie das Kontrollkästchen aller Netzwerk-, Laufwerk- und Computereinstellungen, die bei der Migration erfasst werden sollen.
    - Klicken Sie auf **Dateien und Ordner** und fügen Sie die **Dateien und Ordner** hinzu, die Sie bei der Migration erfassen möchten.
    - Klicken Sie auf **Eigene Dokumente** und bearbeiten Sie die Migrationsregeln für den Ordner "Eigene Dokumente". Diese entsprechen den Regeln für "Dateien und Ordner".
    - Klicken Sie auf **Speichern**, um die Einstellungen in der von Ihnen definierten Befehlsdatei zu speichern.



8. Klicken Sie auf **Speichern**, um das Profilerfassungsskript zu erstellen.

Erstellen eines Skripts für die Profilwiederherstellung

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** auf **Eigene OSD-Skripte** oder **Alle OSD-Skripte**.
3. Klicken Sie auf die Symbolleisten-Schaltfläche für die PE-Umgebung, die Sie verwenden möchten (entweder **Neue DOS PE-Konfiguration** oder **Neue Windows PE-Konfiguration**).
4. Wählen Sie **Profil wiederherstellen** und klicken anschließend auf **OK**.
5. Geben Sie auf der Seite **Allgemein** einen Namen und eine Beschreibung des Skripts ein.
6. Geben Sie auf der Seite **Profil-Datenspeicherung** einen UNC-Pfad und Anmeldeinformationen für die Authentifizierung für das Verzeichnis ein, in dem die Profildaten gespeichert werden sollen. Sie können den Order angeben, in dem das Profil gespeichert ist oder die Option **Die Profildatei auswählen** verwenden und nach der Datei suchen.
    - Geben Sie ein Dateinamensmuster für die Profildaten an. Verwenden Sie eine beliebige Kombination aus Computername, MAC-Adresse und Seriennummer für die Erstellung eines Dateinamens für das Profil. (Wenn Sie beispielsweise **Seriennummer** wählen und die Seriennummer des Geräts lautet 12345678, dann lautet der Profilname "12345678.sma".)
7. Klicken Sie auf **Speichern**, um das Profilwiederherstellungsskript zu erstellen.

Ausführen eines Profilmigrationsskripts

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie im Ordner **Alle OSD-Skripte** das Erfassungs oder Wiederherstellungsskript aus.
3. Klicken Sie auf die Schaltfläche **Planen** in der Symbolleiste.
4. Mit dem Extra **Geplante Tasks** können Sie nun die Ausführung des Skripts auf einem oder mehreren Zielgeräten im Netzwerk planen.

Anpassen der Einstellungen für die Profilmigration

Der Benutzermigrations-Assistent (UMA, User Migration Assistant) speichert Informationen zum Profilinhalt, den Sie migrieren möchten, in einer XML-Datei, die als *Befehlsdatei* bezeichnet wird. Um festzulegen, welche Optionen bei der Erfassung eines Profils gespeichert werden, bearbeiten Sie die Befehlsdatei.

Der einfachste Weg, eine neue Befehlsdatei zu erstellen, besteht darin, ein Profilerfassungsskript im Extra für die Betriebssystembereitstellung zu erstellen. Die von Ihnen hier erstellte Befehlsdatei weist dann die Standardeinstellungen nebst eventueller Änderungen auf, die Sie an den aufgeführten Desktop-, Anwendungs- oder Netzwerkeinstellungen vorgenommen haben.

Wenn Sie die zahlreichen anderen Einstellungen in der Befehlsdatei noch weiter anpassen möchten, können Sie eine neue XML-Datei mit den von Ihnen gewünschten Einstellungen erstellen. Ein Beispiel für eine Befehlsdatei (sample_command_file.xml) finden Sie auf dem Coreserver im Order <Coreserver>\ldlogon\uma\commandxml. Kopieren Sie diese Beispieldatei, wenn Sie benutzerdefinierte Dateien für anderen Profilmigrationstasks erstellen möchten.

In den folgenden Abschnitten finden Sie hilfreiche Informationen dazu, wie Sie eine Befehlsdatei durch Bearbeitung des XML-Dokuments Ihren spezifischen Anforderungen entsprechend anpassen können.

HINWEIS: Wenn Sie eine Befehlsdatei vom Coreserver löschen, werden alle Migrationsskripte, die sich auf diese Befehlsdatei beziehen, nicht mehr ordnungsgemäß ausgeführt. Ferner sollten Sie sämtliche Skripte löschen, die sich auf die Datei beziehen, oder so bearbeiten, dass sie auf eine andere Befehlsdatei verweisen.

Migrieren von Benutzerprofilen

Bei einer Skriptprofilmigration werden standardmäßig alle entdeckten lokalen und Domänenbenutzerkonten auf den Quellgeräten erfasst *mit Ausnahme* der Konten "Alle Benutzer" und "Standardbenutzer".

Alle erfassten Benutzerkonten werden auf den Zielgeräten wiederhergestellt. Ein Benutzerkonto, das noch nicht auf dem Zielgerät vorhanden ist, wird als neues lokales Benutzerkonto erstellt, und seine Einstellungen werden migriert. Vor dem Wiederherstellen von Benutzerkonten können Sie ein Standardkennwort für diese neuen lokalen Benutzerkonten eingeben. Wenn auf dem Zielgerät bereits ein doppeltes Benutzerkonto existiert, werden die erfassten Einstellungen des (Quell-)Benutzerkontos auf das vorhandene Benutzerkonto migriert, das aktuelle Kennwort des Benutzers wird jedoch beibehalten und sollte zum Anmelden verwendet werden.

So legen Sie fest, welche Benutzerprofile migriert werden

Schließen Sie in der UMA-Befehlsdatei im Abschnitt `<IncUsers>` die Benutzernamen aller Benutzer ein, die migriert werden sollen. Sie können alle Benutzer einschließen, indem Sie die Variable `$(all)` verwenden, oder Sie geben die einzelnen Namen jeweils in die Tags `<UserName></UserName>` eingeschlossen ein. Ein Codebeispiel ist nachstehend gegeben.

```
<IncUsers>
<UserName>$(all)</UserName>
</IncUsers>
```

So legen Sie fest, welche Benutzerprofile von der Migration ausgeschlossen werden

Schließen Sie in der UMA-Befehlsdatei im Abschnitt `<ExcUsers>` Benutzernamen von der Migration aus. Geben Sie die einzelnen Namen in die Tags `<UserName></UserName>` eingeschlossen ein. Ein Codebeispiel ist nachstehend gegeben.

```
<ExcUsers>
<UserName>ASPNET</UserName>
</ExcUsers>
```

Migrieren von Desktopeinstellungen

Viele der angepassten und optimierten Einstellungen auf den Desktops Ihrer Geräte können ebenfalls migriert werden. Diese Einstellungen werden in der Befehlsdatei im Abschnitt `<Desktop>` definiert. Geben Sie für jedes Element, das Sie einschließen wollen, `true` innerhalb der Tags an. (Mit `<colors>true</colors>` werden beispielsweise die Farbeinstellungen erfasst.) Für Elemente, die Sie nicht einschließen möchten, geben Sie `false` innerhalb der Tags ein. Sie können eine Auswahl aus folgenden Einstellungen treffen:

- **Desktop Settings (Desktopeinstellungen):** Desktopdesign, Farbschema, visuelle Effekte
- **Accessibility (Eingabehilfen):** Einstellungen für Eingabehilfen, wie beispielsweise die Einstellungen für die Tastatur, den Sound und die Maus (siehe Center für erleichterte Bedienung in der Systemsteuerung von Windows Vista bzw. Windows 7).
- **Active Desktop:** Der aktive Status wird nur beim Betriebssystem Windows 2000 unterstützt.
- **Farben:** Desktop- und Fensterfarben

- **Desktop icons (Desktopsymbole):** Sämtlicher Desktopinhalt, einschließlich Ordnern, Dateien, Shortcuts, Symbolen und der Anordnung der Symbole.
- **Display (Anzeige):** Desktophöhe, -breite und Farbtiefe
- **Icon Font (Schrift für Symbole):** Die für Desktopsymbole verwendete Schrift
- **Tastatur:** Wiederholungsrate der Tastenanschläge, Cursorblinkrate und Verzögerung.
- **Maus:** Einstellungen für links- oder rechtshändige Mausbedienung, Geschwindigkeit und Doppelklickgeschwindigkeit
- **Pattern (Muster):** Das für den Desktop verwendete Muster wird nur beim Betriebssystem Windows 2000 unterstützt.
- **Screen Saver (Bildschirmschoner):** Die aktuellen Einstellungen für den Bildschirmschoner
- **Send To menu (Menü "Senden an"):** Die Einstellungen für das Menü "Senden an"
- **Shell:** Sortierreihenfolge für den Anzeigemodus, Ansichtstyp (große oder kleine Symbole), Statusleiste und der Ein-/Ausblendestatus der Symbolleiste
- **Sound:** Soundeinstellungen
- **Start Menu (Startmenü):** Startmenübefehle
- **Taskbar:** Dockingkante, Größe, Immer im Vordergrund, Automatisch im Hintergrund, Uhr anzeigen, kleine Symbole im Startmenü anzeigen
- **Time zone (Zeitzone):** Zeitzone für das System
- **Wallpaper:** Desktophintergrund
- **Window metrics (Fenstermetrik):** Abstand und Anordnung von minimierten Fenstern, Schrift für Dialognachrichten, Menügröße und Größe der Rollbalken

Folgende Einschränkungen gelten für die Desktopeinstellungen:

- **Active Desktop:** Um den Active Desktop einschließlich Hintergrund zu migrieren, müssen Sie die Einstellung "Hintergrund" ebenfalls auswählen.
- **Symbole:** 1) Die vertikalen und horizontalen Abstände zwischen Desktopsymbolen werden nicht präzise migriert. 2) Nur die Symbole, die sich im Verzeichnis des aktuellen Benutzers befinden, werden migriert.
- **Shell:** Um die Windows Explorer-Shelleinstellungen zu migrieren, müssen Sie sowohl Ihre Shelldesktopeinstellungen als auch Ihre Anwendungseinstellungen für Microsoft Internet Explorer migrieren. Wenn der Zielcomputer Windows 2000 Professional, Windows XP, Windows Vista oder Windows 7 verwendet, werden die Einstellungen für die Ordneransicht (wie z. B. große Symbole, Kacheln und Details) nicht migriert.
- **Sound:** Der Benutzermigrations-Assistent (UMA) migriert das aktive Soundschema vom Quellcomputer auf den Zielcomputer. Das Soundschema wird im Fenster "Sounds und Multimedia - Eigenschaften" der Windows-Systemsteuerung eingestellt. Wenn das Soundschema beim Quellcomputer auf "Keine Sounds" eingestellt ist, werden keine Sounds auf den Zielcomputer migriert. Wenn der Quellcomputer benutzerdefinierte Sounds verwendet, müssen Sie die Audiodateien zusammen mit dem Soundschema migrieren.
- **Wallpaper:** Wenn es sich bei dem Hintergrund, den Sie migrieren möchten, um eine JPEG-Datei handelt, müssen Sie außerdem die Active Desktop-Einstellung erfassen. Wenn Sie einen Hintergrund migrieren, der als BMP-Datei vorliegt, ist es nicht nötig, die Active Desktop-Einstellung zu erfassen.

Ein Codebeispiel für Desktopeinstellungen ist nachstehend gegeben.

```
<Desktop>
<desktop_settings>true</desktop_settings>
```

```
<accessibility>true</accessibility>
<active_desktop>true</active_desktop>
<colors>true</colors>
<desktop_icons>true</desktop_icons>
<display>false</display>
<icon_metrics>false</icon_metrics>
<keyboard>true</keyboard>
<mouse>true</mouse>
<pattern>false</pattern>
<screen_saver>true</screen_saver>
<sendto_menu>false</sendto_menu>
<shell>false</shell>
<sound>true</sound>
<start_menu>false</start_menu>
<taskbar>false</taskbar>
<time_zone>true</time_zone>
<wallpaper>true</wallpaper>
<window_metrics>false</window_metrics>
</Desktop>
```

Migrieren von Anwendungseinstellungen und verknüpften Dateien

Permanente Anwendungseinstellungen und verknüpften Dateien können als Teil eines Geräteprofils migriert werden. Die Anwendungsprogramme selbst werden bei der Profilmigration *nicht* migriert (sie können jedoch zusammen mit dem Betriebssystemabbild bereitgestellt werden).

Einzelne Anwendungen, die migriert werden sollen, werden in der Befehlsdatei im Abschnitt `<Applications>` definiert. Sie können angeben, dass alle Anwendungseinstellungen migriert werden sollen, indem Sie die Variable `$(all)` verwenden.

Der Benutzermigrations-Assistent kann Einstellungen und Anpassungen des Benutzers erfassen. Bei Lotus Notes und Microsoft Outlook könnten diese Einstellungen das Adressbuch und alle lokal gespeicherten E-Mails betreffen. Bei Internet Explorer und Netscape Navigator könnten diese Anpassungen Lesezeichen, Cookies und Einstellungen umfassen.

Ein Codebeispiel für Anwendungseinstellungen ist nachstehend gegeben.

```
<Applications>
<Application>$(all)</Application>
</Applications>
<Inclusions>
<IncDescription>
<Description>%Personal Directory%\ /s</Description>
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
<Operand />
<Size />
</SizeCompare>
<Dest />
<Operation />
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand />
<Date />
</DateCompare>
<SizeCompare>
```

```
<Operand />
<Size />
</SizeCompare>
</ExcDescription>
</Exclusions>
```

Migrieren von Druckereinstellungen

Druckereinstellungen, die migriert werden sollen, werden im Abschnitt <Printers> der Befehlsdatei angegeben. Sie können Einstellungen für einzelne Drucker definieren, indem Sie den Druckernamen in die Tags <Printer> und </Printer> einschließen oder Sie können die Variable $(all) verwenden.

HINWEIS: Sie können nur Druckereinstellungen für Drucker migrieren, für die das von Ihnen verwendete Betriebssystem eingebaute Druckerdefinitionen besitzt.

Einstellungen für virtuelle Drucker (wie beispielsweise für einen XPS-Drucker) können nicht von einem Quellcomputer auf einen Zielcomputer migriert werden.

Ein Codebeispiel für Druckereinstellungen ist nachstehend gegeben.

```
<Printers>
<Printer>$(all)</Printer>
</Printers>
```

Migrieren von Netzwerkeinstellungen

Sie können Einstellungen für Netzwerkverbindungen und -konfigurationen, Computeridentifikation und zugeordnete Laufwerke migrieren. Diese Einstellungen werden in der Befehlsdatei im Abschnitt `<Network>` definiert. Geben Sie für jedes Element, das Sie einschließen wollen, `true` innerhalb der Tags an. (Mit `<computer_name>true</computer_name>` wird beispielsweise der Computername erfasst.) Für Elemente, die Sie nicht einschließen möchten, geben Sie `false` innerhalb der Tags ein. Sie können eine Auswahl aus folgenden Einstellungen treffen:

TCP / IP-Konfiguration

- IP / Subnet / Gateway
- DNS-Konfiguration
- WINS-Konfiguration

Netzwerkidentifikation

- Computername
- Computerbeschreibung
- Domäne / Arbeitsgruppenname

Sonstige

- Freigegebene Ordner / Laufwerke
- Zugeordnete Laufwerke
- DFÜ-Netzwerkverbindung
- Microsoft-Netzwerk
- ODBC-Datenquellen

Folgende Einschränkungen gelten für die Netzwerkeinstellungen:

- **Domäne/Arbeitsgruppe:** Wenn der Quellcomputer Mitglied einer Domäne ist und der Zielcomputer Mitglied derselben Domäne sein soll, erstellen Sie ein Konto für den Zielcomputer auf dem Domänencontroller. Wenn auf dem Domänencontroller Microsoft Windows 2000 Server läuft, wählen Sie die Option **Allow pre-Windows 2000 computers to use this account** (Pre-Windows 2000-Computer dürfen dieses Konto verwenden).
- **DNS-Konfiguration:** Die DNS-Einstellungen werden bei einer PC-nach-PC-Migration nicht migriert.

Ein Codebeispiel für Netzwerkeinstellungen ist nachstehend gegeben.

```
<Network>
<ip_subnet_gateway_configuration>false</ip_subnet_gateway_configuration>
<dns_configuration>false</dns_configuration>
<wins_configuration>false</wins_configuration>
<computer_name>false</computer_name>
<computer_description>false</computer_description>
<domain_workgroup>false</domain_workgroup>
<shared_folders_drives>true</shared_folders_drives>
<mapped_drives>true</mapped_drives>
<dialup_networking>true</dialup_networking>
<microsoft_networking>false</microsoft_networking>
<odbc_datasources>false</odbc_datasources>
</Network>
```

Migrieren von Dateien und Ordnern

Sie können einzelne oder mehrere Dateien migrieren, abhängig vom Speicherort des Verzeichnisses und dem Dateinamen. Einzelne Anwendungen, die migriert werden sollen, werden in der Befehlsdatei im Abschnitt `<FilesAndFolders>` definiert. Sie können einzelne Ordner und Dateien in den Abschnitten `<Inclusions>` und `<Exclusions>` des Dokuments angeben und damit festlegen, welche Dateien eingeschlossen werden sollen ("Inclusions") und welche nicht ("Exclusions").

Geben Sie die Dateien ein, die Sie migrieren möchten. Auf der Seite "Dateien/Ordner" sind die Dateien auf dem Quellcomputer nach Speicherort sortiert aufgeführt. Sie können alle Dateien an einem Speicherort auswählen oder die Struktur erweitern und einzelne Dateien auswählen.

Überlegen Sie sich genau, wo die ausgewählten Dateien auf dem Zielcomputer platziert werden sollen. Wenn die Festplatten auf Quell- und Zielcomputer unterschiedlich konfiguriert sind, müssen Sie alternative Zielorte für Dateien und Verzeichnisse auswählen.

HINWEIS: Seien Sie vorsichtig, wenn Sie die Speicherorte von Dateien ändern. Batchdateien und Konfigurationsdateien enthalten unter Umständen vollqualifizierte Pfadnamen. Wenn Sie die Speicherorte von Dateien und Verzeichnissen ändern, auf die die Batch- und Konfigurationsdateien verweisen, können zugehörige Programme oder Tasks nicht erfolgreich ausgeführt werden.

Ein Codebeispiel für Datei- und Ordnereinstellungen ist nachstehend gegeben.

```
<FilesAndFolders>
<run>true</run>
</FilesAndFolders>
<ArchiveFile>
<filename></filename>
</ArchiveFile>

<Inclusions>
<IncDescription>
<Description>%Personal Directory% /s</Description>
<DateCompare>
<Operand></Operand>
```

```
<Date></Date>
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
<Dest></Dest>
<Operation></Operation>
</IncDescription>
</Inclusions>
<Exclusions>
<ExcDescription>
<Description>%Personal Directory%\*.vol /s</Description>
<DateCompare>
<Operand></Operand>
<Date></Date>
</DateCompare>
<SizeCompare>
<Operand></Operand>
<Size></Size>
</SizeCompare>
</ExcDescription>
</Exclusions>
```

Hilfe zum Betriebssystembereitstellungs- und Profilmigrationsassistenten

In diesem Thema wird der Assistent für Tasks zur Betriebssystembereitstellung/Profilmigration beschrieben.

Hilfe zum Assistenten für Tasks zur Betriebssystembereitstellung/Profilmigration

Der Assistent für Tasks zur Betriebssystembereitstellung/Profilmigration dient zum Erstellen von Skripten, mit denen Betriebssystemabbilder aufgezeichnet oder bereitgestellt und Benutzerprofile aufgezeichnet oder wiederhergestellt werden. Nachdem Sie Skripte erstellt haben, können Sie einen Zeitplan für die Verteilung dieser Skripte erstellen, die als Task auf Zielgeräten in Ihrem Netzwerk ausgeführt werden. Der Assistent wird entweder über die betreffende Schaltfläche in der Symbolleiste oder über die Kontextmenüs im Extra "Betriebssystembereitstellung" (**Extras > Verteilung > Betriebssystembereitstellung**) aufgerufen.

HINWEIS: Hier werden sämtliche Seiten des Assistenten für Tasks zur Betriebssystembereitstellung/Migration beschrieben. Welche Seiten während der Ausführung des Assistenten tatsächlich angezeigt werden, hängt jedoch vom jeweiligen Abbilderstellungs (Imaging)- oder Migrationstask ab, den Sie beim Start des Assistenten ausgewählt haben.

Auswählen eines Skripttyps

Zu Beginn geben Sie auf der Basis der folgenden Tasks an, welche Art von Skript für die Betriebssystembereitstellung/Profilmigration erstellt werden soll:

- **Abbild erfassen:** Erstellt ein Skript, das ein Betriebssystemabbild von einem Gerät erstellt und speichert. Abbilder können mithilfe des integrierten LANDesk Abbilderstellungstools (ImageW) oder mit einem Tool eines anderen Herstellers, z. B. mit Microsoft ImageX oder Symantec Ghost, aufgezeichnet werden.

- **Profil erfassen:** Erstellt ein Skript, das die einem Gerät eigenen Benutzereinstellungen, Anwendungs- und Desktop-Einstellungen sowie Dateien erfasst. Mit dieser Option können Sie auch auf das Dialogfeld "Sammlungsmanager" zugreifen, um ein vom Benutzer initiiertes Profilmigrationspaket zu erstellen, das lokal auf einzelnen Geräten ausgeführt werden kann.
    - **Mit File-Capture-Fehlern fortfahren:** Lässt zu, dass die Profilerfassung fortgesetzt wird, selbst wenn zu erfassende Dateien Dateifehler melden (beispielsweise ungültige Dateinamen, gesperrte Dateien oder Dateien, die ihre Größe während des Erfassungsvorgangs ändern). Die Profilerfassung wird abgeschlossen und Dateifehler werden in der Protokolldatei aufgezeichnet.
- **Abbild bereitstellen:** Erstellt ein Skript, das ein zuvor erstelltes Betriebssystemabbild auf Zielgeräte bereitstellt.
- **Profil wiederherstellen:** Erstellt ein Skript, das zuvor erfasste Profildaten auf Zielgeräten wiederherstellt (Benutzereinstellungen, Anwendungs- und Desktop-Einstellungen sowie Dateien).

Neues generisches DOS-Taskskript

Mit dieser Schaltfläche der Symbolleiste wird ein Skript erstellt, das auf Geräten DOS-Befehle ausführt (einschließlich Anwendungsstart).

Informationen zur Seite "Allgemein"

Auf dieser Seite konfigurieren Sie die folgenden Merkmale eines Betriebssystem-Abbilderstellungstasks:

- **Name:** Bezeichnung des Skripts durch einen eindeutigen Namen. Falls der hier eingegebene Name bereits verwendet wird, werden Sie aufgefordert zu bestätigen, dass das vorhandene Skript ersetzt werden soll. Geben Sie einen Namen ein, der es Ihnen leicht macht, das Skript anhand seiner Funktion oder der vorgesehenen Zielgeräte im Netzwerk rasch und mühelos zu identifizieren.
- **Beschreibung** (optional) Zusätzlicher Text, der das Skript beschreibt.
- **Mit File-Capture-Fehlern fortfahren:** Lässt zu, dass die Profilerfassung fortgesetzt wird, selbst wenn zu erfassende Dateien Dateifehler melden (beispielsweise ungültige Dateinamen, gesperrte Dateien oder Dateien, die ihre Größe während des Erfassungsvorgangs ändern). Die Profilerfassung wird abgeschlossen und Dateifehler werden in der Protokolldatei aufgezeichnet.

HINWEIS: Wenn Sie dieses Skript dem LANDesk PXE-DOS-Menü hinzufügen, wird die hier eingegebene Beschreibung im Menü angezeigt.

Informationen zum Dialogfeld "Abbild erfassen" – Seite "Anmeldeinformationen"

Verwenden Sie diese Seite, um die Anmeldeinformationen für die Authentifizierung für den oder die freigegebenen Netzwerkordner bereitzustellen, in dem/in denen das Betriebssystemabbild und das Abbilderstellungstool, mit dem das Abbild erstellt wurde, gespeichert wurden.

HINWEIS: Sie können lediglich einen Satz Anmeldeinformationen eingeben. Da dieser Satz für den Zugriff auf beide Freigaben verwendet wird, müssen die Anmeldeinformationen für diese Freigaben übereinstimmen. Die Anmeldeinformationen müssen einem lokalen Benutzerkonto auf dem Gerät gehören, das als Host für die Freigabe dient.

- **Domäne\Benutzername:** Identifiziert ein Benutzerkonto, das über die Anmeldeinformationen verfügt, die für die Anmeldung bei der Netzwerkfreigabe erforderlich sind.

- **Kennwort/Kennwort bestätigen:** Geben Sie das Kennwort des Benutzers ein und bestätigen Sie es.

Informationen zum Dialogfeld "Abbild aufzeichnen" – Seite "Abbilddaten"

Auf dieser Seite geben Sie an, welcher Abbildtyp mit diesem Skript erstellt werden soll, wo das Abbild gespeichert wird und im welchem Verzeichnis sich das Abbilderstellungstool befindet.

- **Abbildtyp:** Bezeichnung des Dateityps (Formats) der Abbilddatei, die mit diesem Skript erstellt wird; der Dateityp wird durch die Auswahl eines Tools aus der Liste der Abbilderstellungstools festgelegt.
- **Geben Sie das UNC-Pfadverzeichnis ein:** Bezeichnung des Servers und der Freigabe, die als Speicherort der Abbilddatei dienen sollen. Das Abbild muss in einem freigegebenen Ordner gespeichert werden, auf den Geräte zugreifen können. Beachten Sie, dass der Freigabename keine Leerzeichen enthalten darf. Sie können den Gerätenamen einfach im UNC-Format angeben und dann die restliche Pfadangabe ergänzen, indem Sie auf die Schaltfläche "Durchsuchen" klicken und die Freigabe suchen. In einigen Fällen wird beim Suchen nach einem Pfad ein lokaler Pfad eingefügt. Sie müssen diesen Pfad in das UNC-Format konvertieren.

HINWEIS: Während der Abbilderstellung ordnen Geräte diesen UNC-Pfad dem Laufwerk I: zu.

- **Geben Sie den UNC-Pfad zur Abbilderstellungsanwendung ein:** Gibt den Server und die Freigabe an, die als Speicherort für das Abbilderstellungstool (das dem oben ausgewählten Abbildtyp entspricht) dienen, einschließlich des Namens der ausführbaren Datei des Tools. Beachten Sie, dass der Freigabename keine Leerzeichen enthalten darf. In einigen Fällen wird beim Suchen nach einem Pfad ein lokaler Pfad eingefügt. Sie müssen diesen Pfad in das UNC-Format konvertieren.

HINWEIS: Während der Abbilderstellung ordnen Geräte diesen UNC-Pfad dem Laufwerk H: zu.

- **Partition auswählen:** (Nur für Windows PE-Abbilder) Hiermit können Sie die Partition auswählen, in der auf dem verwalteten Gerät das Abbild bereitgestellt werden soll. Die von Ihnen ausgewählte Partition wird zum Laufwerk C.

Informationen zum Dialogfeld "Abbild erfassen" – Seite "Zusätzliche Befehle"

Verwenden Sie diese Seite, um das Skript durch Hinzufügen von benutzerdefinierten Befehlen anzupassen.

- **Befehle eingeben, die vor dem Neustart und der Abbilderstellung des Geräts ausgeführt werden sollen:** Dieses Textfeld akzeptiert zusätzliche Befehle, wobei Sie diese wie an einer Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen. Die einzelnen Befehle werden nacheinander an die Geräte gesendet. Diese Befehle werden nach dem Neustart und der Abbilderstellung des Geräts ausgeführt.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Methoden und Anmeldeinformationen"

Verwenden Sie diese Seite, um die Anmeldeinformationen für die Authentifizierung für den oder die freigegebenen Netzwerkordner bereitzustellen, in dem bzw. denen das Betriebssystemabbild und das Abbilderstellungstool, mit dem das Abbild erstellt wurde, gespeichert wurden.

- **Multicastdownload:** Verwendet in den Subnetzen Ihres Netzwerks enthaltene Multicast-Domänenrepräsentanten, um das Betriebssystemabbild mithilfe der LANDesk Targeted Multicast-Technologie bereitzustellen. Mithilfe der Multicasting-Technologie können Sie Softwarepakete gleichzeitig an mehrere Geräte verteilen, wodurch der erforderliche Zeit- und Bandbreitenaufwand beträchtlich verringert wird. Statt für jedes Gerät ein Paket über das Netzwerk zu senden, wird für jedes Subnetz nur eine Übertragung durchgeführt.

HINWEIS: Bevor Sie Multicasting verwenden, müssen Sie sicherstellen, dass die Multicasting-Komponenten in dem Subnetz vorhanden sind, an das Pakete verteilt werden. Für Targeted Multicasting werden LANDesk Management Suite Agenten ab Version 6.62 und ein LANDesk Management Suite Multicast-Domänenrepräsentant ab Version 6.62 benötigt.

- **Abbild wird von SysPrep verarbeitet:** Gibt an, dass Sie das bereitzustellende Betriebssystemabbild mit Microsoft SysPrep konfiguriert haben. Wenn Sie diese Option auswählen, können Sie auf einer nachfolgenden Seite des Assistenten SysPrep-Dateiinformationen und -Bereitstellungsoptionen angeben.
- **Hardwareunabhängige Abbilderstellung verwenden:** Wählen Sie diese Option aus, wenn Sie das Extra "Hardwareunabhängige Abbilderstellung" in den Abbilderstellungsprozess einbeziehen möchten. Mit diesem Extra können Sie ein elementares Abbild definieren, das auf mehrere Gerätemodelle angewendet werden kann und dann auf der Basis des Geräteherstellers und Modells Treiber für jedes Gerät injiziert. Wenn Sie diese Option auswählen, müssen Sie ferner im Abschnitt **SysPrep-Optionen** hardwareunabhängige Abbildoptionen definieren.
- **Profilmigration einbeziehen:** Bindet sowohl Profilerfassungs- als auch Profilwiederherstellungsprozesse in den Abbildbereitstellungsauftrag ein. Wenn Sie diese Option auswählen, können Sie auf einer nachfolgenden Seite des Assistenten Profilmigrationsoptionen angeben.

HINWEIS: Sie können lediglich einen Satz Anmeldeinformationen eingeben. Da dieser Satz für den Zugriff auf beide Freigaben verwendet wird, müssen die Anmeldeinformationen für diese Freigaben übereinstimmen. Die Anmeldeinformationen müssen einem lokalen Benutzerkonto auf dem Gerät gehören, das als Host für die Freigabe dient.

- **Domäne\Benutzername:** Identifiziert ein Benutzerkonto, das über die Anmeldeinformationen verfügt, die für die Anmeldung bei der Netzwerkfreigabe erforderlich sind.
- **Kennwort/Kennwort bestätigen:** Geben Sie das Kennwort des Benutzers ein und bestätigen Sie es.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Multicast-Erkennung"

Auf dieser Seite konfigurieren Sie die folgenden grundlegenden Targeted Multicasting-Optionen für ein Abbildverteilungsskript:

- **Multicast-Domänenerkennung verwenden:** Bevor die Targeted Multicasting-Technologie zum Bereitstellen von Abbildern auf Geräten in Ihrem Netzwerk eingesetzt wird, wird in Subnetzen Ihres Netzwerks nach Multicast-Domänenrepräsentanten gesucht.
- **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Sucht vor dem Bereitstellen des Abbilds in den Subnetzen Ihres Netzwerks nach Multicast-Domänenrepräsentanten und speichert die Ergebnisdaten, um künftige Targeted Multicasting-Bereitstellungen zu vereinfachen.

HINWEIS: Es werden jeweils nur die Ergebnisse eines Suchlaufs der Multicast-Domänenerkennung gespeichert; wenn Sie diese Option für ein Abbildbereitstellungsskript auswählen, werden daher die Ergebnisse der vorherigen Multicast-Domänenerkennung überschrieben.

- **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwendet bei der Abbildbereitstellung auf Geräten die neueste Liste mit erkannten Multicast-Domänenrepräsentanten.

  Wählen Sie diese Option *nur dann* aus, wenn Sie die Ergebnisdaten einer Multicast-Domänenerkennung schon mindestens einmal gespeichert haben.

- **Erweiterte Multicast-Optionen konfigurieren:** Hiermit können Sie das Verhalten von Targeted Multicasting für ein Bereitstellungsskript noch genauer anpassen, indem Sie auf der nächsten Seite des Assistenten erweiterte Multicast-Optionen konfigurieren.
- **Domänenrepräsentanten reaktivieren verwaltete Geräte:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan"-Technologie unterstützen, beim Empfang von Multicast reaktivieren möchten. Mit dem Dialogfeld "Multicast-Optionen" können Sie festlegen, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das "Wake on Lan"-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden.
- **Wartezeit nach WOL-Versuch (Sek.):** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Erweiterte Optionen"

Auf dieser Seite konfigurieren Sie die folgenden erweiterten Targeted Multicasting-Optionen für ein Abbildverteilungsskript:

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Bestimmt die Höchstzahl von Multicast-Domänenrepräsentanten, die gleichzeitig unter Verwendung der Targeted Multicasting-Technologie ein Abbild aktiv bereitstellen können.
- **Speicherzeitraum für Dateien im Geräte-Cache:** Legt die Zeitspanne fest, über die das per Multicasting verteilte Abbild im lokalen Cache der einzelnen Zielgeräte verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Speicherzeitraum für Dateien im Cache des Multicast-Domänenrepräsentanten:** Legt die Zeitspanne fest, über die das per Multicasting verteilte Abbild im Cache der Multicast-Domänenrepräsentanten verbleiben kann. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Prozentsatz der vom Core oder bevorzugten Server genutzten Bandbreite (WAN):** Steuert, welcher Prozentanteil der verfügbaren Bandbreite verwendet wird, wenn nicht der Multicast-Domänenrepräsentant das Multicasting einer Datei aus dem eigenen Cache durchführt, sondern der Coreserver oder der bevorzugte Server verwendet wird. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.
- **Prozentsatz der Peer-zu-Peer genutzten Bandbreite (lokal):** Steuert, wie viel Prozent der verfügbaren Bandbreite bei Verwendung eines Peer-to-Peer-Multicast genutzt wird.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Abbildtyp und -pfad"

Auf dieser Seite geben Sie an, welcher Abbildtyp mit diesem Skript wiederhergestellt werden soll, wo das Abbild gespeichert wird und in welchem Verzeichnis sich das Abbilderstellungstool befindet.

- **Abbildtyp:** Bezeichnung des Dateityps (Formats) der vorhandenen Abbilddatei, die mit diesem Skript bereitgestellt werden soll; der Dateityp wird durch die Auswahl eines Tools aus der Liste der Abbilderstellungstools festgelegt.
- **Geben Sie das UNC-Pfadverzeichnis ein:** Gibt den Server und die Freigabe an, die als Speicherort für die Abbilddatei dienen, einschließlich des Dateinamens des Abbilds. Das Abbild muss in einem für Geräte zugänglichen freigegebenen Ordner gespeichert werden.
- **Geben Sie den UNC-Pfad zur Abbilderstellungsanwendung ein:** Gibt den Server und die Freigabe an, die als Speicherort für das Abbilderstellungstool (das dem oben ausgewählten Abbildtyp entspricht) dienen, einschließlich des Namens der ausführbaren Datei des Tools.
- **Partition auswählen:** (Nur für Windows PE-Abbilder) Hiermit können Sie die Partition auswählen, in der auf dem verwalteten Gerät das Abbild bereitgestellt werden soll. Die von Ihnen ausgewählte Partition wird zum Laufwerk C.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Zusätzliche Extra-Befehle"

Wenn Sie Powerquest als Abbilderstellungstool verwenden, können Sie auf dieser Seite zusätzliche "Powerquest-Befehle" hinzufügen. Die Seite ist nicht verfügbar, wenn Powerquest von Ihnen nicht ausgewählt wurde.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Preboot-Befehle"

Verwenden Sie diese Seite, um das Skript durch Hinzufügen von benutzerdefinierten Befehlen anzupassen.

- **Geben Sie Befehle ein, die vor dem Neustart und vor der Abbilderstellung des Geräts ausgeführt werden sollen:** Dieses Textfeld akzeptiert zusätzliche Befehle, wobei Sie diese wie an einer Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen. Die einzelnen Befehle werden nacheinander an die Geräte gesendet. Diese Befehle werden vor dem Neustart und der Abbilderstellung des Geräts ausgeführt.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "SysPrep-Optionen"

Verwenden Sie diese Seite, um folgende Informationen zur Sysprep-Datei (Sysprep.inf) zur Verfügung zu stellen, die von diesem Skript zum Ändern des zur Bereitstellung anstehenden Abbilds verwendet wird:

- **Windows-Produkt auswählen:** Wählen Sie die Windows-Version aus, die Sie für SysPrep verwenden werden.

- **Vorhandene SYSPREP-Datei als Vorlage verwenden:** Verwendet eine vorhandene Sysprep.inf-Datei als Vorlage für eine neue Datei und gibt an, wo die vorhandene Datei gespeichert wurde. Die neue Sysprep.inf-Datei, die die in diesem Assistenten vorgenommenen Einstellungen enthält, überschreibt die vorhandene Sysprep-Standarddatei. Wenn die Betriebssystembereitstellung die Sysprep.inf-Datei auf der Grundlage einer von Ihnen erstellten Datei anlegen soll, dann können Sie nach dieser Datei suchen. Falls Sie keine vorhandene Sysprep.inf-Datei auswählen, wird von der Betriebssystembereitstellung eine neue Datei erstellt.

HINWEIS: Nachdem Sie den Assistenten ausgeführt haben, können Sie die mit einem Skript assoziierte sysprep.inf bearbeiten, indem Sie mit der rechten Maustaste auf das Skript und dann auf **Erweiterte Bearbeitung** klicken.

- **Sysprep.inf-Speicherort des bereitgestellten Abbildes:** Angabe des Speicherorts, an dem sich die Datei Sysprep.inf auf der Festplatte des Geräts befand, auf dem Sysprep ursprünglich ausgeführt wurde (d. h. das Gerät, dessen Abbild mit diesem Skript bereitgestellt wird).
- **Erweiterte Multiprozessoroptionen konfigurieren:** Mit dieser Option können Sie ein Abbild zur Unterstützung von Multiprozessorsystemen konfigurieren.

HINWEIS: Wählen Sie diese Option nur dann aus, wenn sich die Prozessoranzahl im Abbild von der Prozessoranzahl eines Ihrer Zielgeräte unterscheidet.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Multiprozessor"

Auf dieser Seite konfigurieren Sie die folgenden Multiprozessor-Einstellungen für das Abbild, das mit diesem Skript bereitgestellt wird:

- **Den Betriebssystemtyp für das bereitgestellte Abbild eingeben:** Geben Sie das Betriebssystem an, das zu dem Abbild gehört, das bereitgestellt wird.
- **Geben Sie den Gerätetyp an, auf dem das Abbild erstellt wurde:** Gibt an, ob das bereitzustellende Abbild auf einem Einzelprozessor- oder einem Multiprozessorgerät mit APIC oder MPS-Architektur erstellt wurde.
- **Geben Sie den Ort der HAL-bezogenen .inf-Dateien im Abbild ein:** Gibt den Pfad der HAL-bezogenen .inf-Datei für das Abbild an, das mit diesem Skript bereitgestellt wird. Der Assistent verwendet standardmäßig für jedes Betriebssystem die von Microsoft definierten .inf-Standarddateipfade. Wenn Sie bei der Konfiguration des Gerät für die Abbilderstellung die Standardpfade verwendet haben, übernehmen Sie die Angaben in diesem Textfeld. Andernfalls geben Sie den hiervon abweichenden Pfad ein, den Sie für die HAL-bezogene .inf-Datei benutzt haben.

Zusätzliche Multiprozessordaten

Einzelprozessor- und Multiprozessorgeräte benötigen unterschiedliche Windows-Kernel. Je nach Hardwarekonfiguration können Sie möglicherweise ein für ein Einzelprozessorsystem erstelltes Abbild auch auf einem Multiprozessorgerät verwenden oder umgekehrt.

Geräte, die erweiterte Prozessorfunktionen unterstützen, verfügen in der Regel über einen Advanced Programmable Interrupt Controller (APIC). Geräte, die erweiterte Prozessorfunktionen unterstützen, können zudem mit einer Advanced Configuration and Power Interface (ACPI)-Schnittstelle ausgestattet sein.

Die Bedingungen, unter denen ein Abbild sowohl für Einzelprozessor- als auch Multiprozessorgeräte verwendet werden kann, sind kompliziert. Detaillierte Informationen hierzu finden Sie in der Sysprep-Dokumentation von Microsoft.

WARNUNG: Grundsätzlich ist bei der gemeinsamen Nutzung von Einzelprozessor- und Multiprozessorabbildern zu beachten, dass sowohl Quell- als auch Zielgeräte entweder eine APIC-HAL mit ACPI-Unterstützung oder eine APIC-HAL ohne ACPI-Unterstützung besitzen müssen. Sie können auf einem APIC-Gerät ohne ACPI-Unterstützung kein ACPI-APIC-Abbild verwenden und umgekehrt auf einem ACPI-APIC-Gerät kein APIC-Abbild ohne ACPI-Unterstützung.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Abbildeinstellungen"

Auf dieser Seite geben Sie die folgenden allgemeinen Einstellungen für die Datei Sysprep.inf an, die von diesem Skript verwendet wird, um das zur Bereitstellung anstehende Abbild zu modifizieren:

- **Zeitzone:** Gibt an, in welcher Zeitzone sich die Zielgeräte befinden.
- **Datenträgerlizenzschlüssel:** Gibt die Lizenznummer des zur Bereitstellung anstehenden Betriebssystems an.
- **Lokales Administratorkennwort für dieses Abbild:** Gibt das Administratorkennwort für das Gerät an, auf dem das Abbild erstellt wurde.
- **Name:** Identifiziert die Zielgeräte anhand eines Namens, beispielsweise dem Namen einer Abteilung oder eines geografischen Standorts.
- **Organisation:** Identifiziert Ihre Organisation anhand eines Namens, beispielsweise dem Namen eines Geschäftsbereichs oder einem Firmennamen.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Netzwerk-Anmeldeinformationen"

Auf dieser Seite legen Sie die folgenden Netzwerkeinstellungen fest, die in die Sysprep.inf-Datei dieses Abbilds aufgenommen werden sollen:

- **Arbeitsgruppe:** Gibt an, dass die Zielgeräte Mitglieder einer Arbeitsgruppe sind. Wenn Sie diese Option auswählen, müssen Sie den Namen der Arbeitsgruppe in das Textfeld eingeben.
- **Domäne:** Gibt an, dass die Zielgeräte Mitglieder einer Domäne sind. Wenn Sie diese Option auswählen, müssen Sie den Namen der Domäne in das Textfeld eingeben und die folgenden Informationen zu Domänenkonten bereitstellen:
  - **Domänenbenutzername:** Identifiziert den Namen eines Domänenbenutzers, der zum Hinzufügen eines Rechnerkontos zu dieser Domäne berechtigt ist.
  - **Domänenkennwort:** Stellt das Kennwort des Benutzers bereit.
  - **Gerät einer ActiveDirectory-Organisationseinheit hinzufügen:** Gibt Ihnen die Möglichkeit (unter Verwendung der LDAP-Pfadsyntax), den Pfad einer bestimmten Microsoft Active Directory-Organisationseinheit anzugeben, der die abzubildenden Zielgeräte hinzugefügt werden sollen.
  - **Name der Organisationseinheit (OE):** Geben Sie den Namen der Organisationseinheit ein.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Benennungskonvention"

Auf dieser Seite weisen Sie die Namenskonvention für die Zielgeräte zu, die durch das Abbildbereitstellungsskript abgebildet werden.

- **Erst versuchen, vorhandene Computernamen aus der Inventardatenbank abzurufen und zu verwenden:** Mit dieser Option werden vorhandene Windows-Computernamen beibehalten, falls die Zielgeräte bereits vom Inventarscanner erfasst wurden. Das Abbild versucht dann, bereits in der Coredatenbank vorhandene Computernamen zu verwenden.
- **Verwenden Sie, falls notwendig, die folgende Vorlage zur Benennung der Zielcomputer:** Stellt eine Vorlage zur Verfügung, die eine Namenskonvention zur Erstellung eindeutiger Namen für diejenigen Zielgeräte definiert, denen in der Coredatenbank bisher noch kein Gerätename zugeordnet wurde. Diese Vorlage ist nützlich für von der LANDesk-Agentenerkennung ermittelte und mit der PXE-Startoption gebootete Geräte. Sehen Sie sich hierzu die Beispiele auf der betreffenden Seite des Assistenten an.
- **Startnummer:** Geben Sie die Nummer ein, die mit der oben eingegebenen Vorlage verknüpft ist. Die Betriebssystembereitstellung verwaltet einen fortlaufenden Zähler der verwendeten Nummern. So werden nachfolgende Aufträge dort fortgesetzt, wo der letzte Auftrag endete. Jede eindeutige Vorlage besitzt einen eigenen Zähler. Wenn Sie immer dieselbe Vorlage verwenden, umfasst der Zähler verschiedene Aufträge. Markieren Sie das Kontrollkästchen **Vorhandenen Wert beim Speichern überschreiben**, um die vorhandene Nummer mit der unter **Startnummer** eingegebenen Nummer zu ersetzen.

Informationen zum Dialogfeld "Abbild bereitstellen" – Seite "Hardwareunabhängige Abbilderstellung"

Diese Seite verwenden Sie zur Konfiguration der Verwendung der hardwareunabhängige Abbilderstellung (HII, hardware-independent imaging) in einem Skript. Mit dem Extra zur hardwareunabhängigen Abbilderstellung (hiiclient.exe) können Sie eine einzige Versorgungsvorlage bzw. ein Bereitstellungsskript erstellen und auf mehreren Gerätemodellen bereitstellen. Auf dem Gerät wird zunächst ein Basisabbild installiert, und das HII-Extra injiziert dann die für dieses Gerätemodell spezifischen Treiber.

Diese Option kommt nur bei Abbildern zum Einsatz, die auf der Windows-Prebootumgebung basieren. Nach der Installation des Betriebssystems, aber noch vor dem Neustart des Geräts, erkennt das HII-Extra das Gerätemodell und ruft Treiber für dieses Modell ab. Die Treiber werden auf dem Gerät installiert und die zugehörigen Information werden in die Registry aufgenommen. Wenn das Betriebssystem dann nach einen Neustart hochfährt, werden die Treiber konfiguriert.

- **UNC zum Kopieren von Treiberdateien verwenden:** Aktivieren Sie diese Option, wenn Sie ausschließlich UNC-Adressierung für den Zugriff auf das Gerätetreiber-Repository verwenden möchten. Wenn Sie diese Option nicht auswählen, kann auch HTTP für den Zugriff auf die Treiber verwendet werden.

Informationen zu "Abbild bereitstellen" – Seite "LANDesk Agent"

Auf dieser Seite geben Sie die folgenden Informationen ein, die das Abbild benötigt, um die LANDesk Gerätesoftware auf den Zielgeräten installieren zu können.

- **UNC-Pfad zum Verzeichnis, das wscfg32.exe enthält:** Angabe des UNC-Pfads (normalerweise \\<Corename>\LDLogon) zum Coreserver oder Service Center, in dem WSCFG32.EXE (die

LANDesk-Geräte-Setupdatei) gespeichert ist.

- **LANDesk Anmeldeinformationen für den Zugriff auf den Coreserver:** Stellt einen Domänen-/Benutzernamen, ein Kennwort und ein bestätigtes Kennwort für die Authentifizierung gegenüber dem Coreserver oder Service Center zur Verfügung, damit das Abbild die Datei wscfg32.exe auf den Zielgeräten installieren kann.

Informationen zum Dialogfeld "Profil erfassen" – Seite "UNC-Datenspeicherung"

Die Optionen auf dieser Seite werden auch auf der Seite **Profil-Datenspeicherung** des Dialogfeldes "Abbild bereitstellen und Profil wiederherstellen" angezeigt. Auf dieser Seite geben Sie an, wo die Profildaten gespeichert und die Anmeldeinformationen für die Authentifizierung zur Verfügung gestellt werden sollen.

- **Wählen Sie die wiederherzustellende UNC aus:** (Nur bei "Profil erfassen") Gibt den UNC-Pfad für den Speicherort der Profildaten an. Sie können den Computernamen einfach im UNC-Format angeben und dann die restliche Pfadangabe ergänzen, indem Sie auf die Schaltfläche "Durchsuchen" klicken.
- **Den Profilordner auswählen:** (Nur bei "Profil wiederherstellen") Klicken Sie hier, um den Ordner auszuwählen, in dem sich die Datei befindet. Geben Sie den Speicherort des Ordners ein oder klicken Sie auf "Durchsuchen", um ihn zu finden.
- **Die Profildatei auswählen:** (Nur bei "Profil wiederherstellen") Klicken Sie hier, um das Profil auszuwählen. Geben Sie Pfad und Namen des Profils ein oder klicken Sie auf Durchsuchen, um es zu finden.
- **Dateinamenoptionen:** (Profil erfassen) Wählen Sie die Option aus, mit der Sie das Profil speichern möchten. Sie können **Computername**, **MAC-Adresse** und/oder **Seriennummer** wählen. Wenn Sie beispielsweise "Seriennummer" wählen und die Seriennummer des Geräts lautet 12345678, dann wird der Profilname als "12345678.sma" gespeichert.

  (Profil wiederherstellen) Wählen Sie die Option, die dem Profil im ausgewählten Profilordner entspricht. Sie können **Computername**, **MAC-Adresse** und/oder **Seriennummer** wählen. Wenn Sie beispielsweise "MAC-Adresse" wählen und die MAC-Adresse lautet "0013207f7da2", dann sollte das Profil mit dem Namen "0013207f7da2.sma" aus dem Profilordner zum Wiederherstellen des Profils verwendet werden. Vergewissern Sie sich, dass der ausgewählte Profilordner auch tatsächlich die Profildatei mit dem richtigen Namen enthält, sonst schlägt dieser Task fehl.
- **Domäne\Benutzername:** Angabe eines Benutzers, der für den angegebenen UNC-Pfad über gültige Anmeldeinformationen für die Authentifizierung verfügt.
- **Kennwort/Kennwort bestätigen:** Gibt das Kennwort des Benutzers an.
- **Authentifizierung unter Verwendung dieser Anmeldeinformationen erzwingen:** Erzwingt auf Geräten, für die eine Profilmigration geplant wurde, eine Authentifizierung (Abmelden und Anmelden unter Verwendung der oben angegebenen Anmeldeinformationen), wenn die Anmeldeinformationen des gegenwärtig angemeldeten Benutzers nicht ausreichen. Wenn ein solcher Fehler auftritt, kann durch die Auswahl dieser Option sichergestellt werden, dass das Gerät über die erforderlichen Rechte zum Lesen und Speichern von Daten auf der Netzwerkfreigabe verfügt, unter der die Profildaten gespeichert werden.

Informationen zu "Profil erfassen" – Seite "UMA-Befehlsdatei"

Diese Seite verwenden Sie, um den Speicherort der UMA-Befehlsdatei anzugeben, die zur Erfassung von Benutzerprofilen verwendet wird. Bei dieser Befehlsdatei handelt es sich um eine XML-Datei, die festlegt, welche Elemente in dem zu erfassenden Profil eingeschlossen werden sollen. Auf dieser Seite können Sie ferner die gängigsten Elemente in der UMA-Befehlsdatei bearbeiten, ohne die Datei zu öffnen und den XML-Code direkt bearbeiten zu müssen.

- **XML-Befehlsdatei des Benutzermigrations-Assistenten auswählen:** Klicken Sie auf **Durchsuchen** und wählen Sie den Speicherort der XML-Datei aus.
- **Bearbeiten:** Klicken Sie auf diese Schaltfläche, um das Dialogfeld **Migrationseinstellungen auswählen** zu öffnen. Wählen Sie die UMA-Befehlsdatei aus, die Sie bearbeiten möchten und klicken Sie auf die Schaltfläche **Bearbeiten**. Sie können auch eine neue Befehlsdatei erstellen, indem Sie auf **Neu** klicken.
    - **Speichern:** Geben Sie den Namen der XML-Datei an.
    - **Desktopeinstellungen:** Markieren Sie das Kontrollkästchen für jedes Desktopelement, das Sie in dem Profil erfassen möchten.
    - **Anwendungseinstellungen:** Markieren Sie das Kontrollkästchen für jede Anwendung, für die Sie die Benutzereinstellungen in dem Profil erfassen möchten.
    - **Netzwerkeinstellungen:** Markieren Sie das Kontrollkästchen für jede Netzwerk- und Laufwerkseinstellung, die Sie in dem Profil erfassen möchten.

Weitere Informationen zur Profilmigration und zur UMA-Befehlsdatei finden Sie unter "Übersicht über die Profilmigration" auf Seite 402"Übersicht über die Profilmigration" auf Seite 402

Informationen zur Seite "Allgemein" des Skripteditors für DOS-Task

Auf dieser Seite können Sie ein Skript erstellen, das DOS-Befehle (einschließlich Namen von Anwendungsprogrammdateien) auf Zielgeräten ausführt. Die einzelnen Befehle werden nacheinander an die Geräte geschickt.

- **Name:** Bezeichnung des Skripts durch einen eindeutigen Namen. Falls der hier eingegebene Name bereits verwendet wird, werden Sie aufgefordert zu bestätigen, dass das vorhandene Skript ersetzt werden soll. Geben Sie einen Namen ein, der es Ihnen leicht macht, das Skript anhand seiner Funktion oder der vorgesehenen Zielgeräte im Netzwerk rasch und mühelos zu identifizieren.
- **Beschreibung** (optional) Zusätzlicher Text, der das Skript beschreibt.
- **Die DOS-Befehle für die Ausführung auf diesem Gerät eingeben:** In dieses Textfeld können DOS-Befehle eingefügt werden, wobei Sie diese wie an der DOS-Eingabeaufforderung jeweils in einer eigenen Zeile eingeben müssen. Sie können beliebig viele Befehle eingeben.
- **Diesen Auftrag abbrechen, wenn ein Befehl fehlschlägt:** Bewirkt, dass der Abbilderstellungsauftrag abgebrochen wird, falls einer der auf dieser Seite eingegebenen DOS-Befehle fehlschlägt. Von der DOS-Befehlszeile gestartete Anwendungen, die im Fehlerfall einen DOS-Errorlevel-Code generieren, können ebenfalls den Abbruch des Abbilderstellungsauftrags bedingen. Wenn beim Scheitern eines Befehls oder einer Anwendung kein Errorlevel-Code generiert wird, wird der Abbilderstellungsauftrag weiter ausgeführt.

Überprüfen der Gültigkeit von Bootumgebungen für die Betriebssystembereitstellung

Die Bootumgebungen für die Betriebssystembereitstellung können verwendet werden, sobald Sie Ihre Lizenz für die Verwendung validiert haben.

In einer DOS PE-Bootumgebung muss die Betriebssystembereitstellung überprüfen, ob Sie die Lizenz besitzen, die es Ihnen ermöglicht, die für die Bootumgebung erforderlichen Dateien zu verwenden. Die Lizenzverifizierung erfordert eine Windows NT 4 Server- und eine Windows 98-CD.

Windows PE wird im Rahmen der Installation von Management Suite für Sie installiert. Das LANDesk PE-Toolkit verwendet die Microsoft Windows Pre-installation Environment Software ("WinPE"), bei der es sich um ein Drittanbieterprodukt handelt. Damit Sie das LANDesk PE Toolkit verwenden können, müssen Sie die Microsoft WinPE-Lizenzvereinbarung akzeptiert haben. Klicken Sie die Schaltfläche **Lizenz**, um zu beginnen.

Hinzufügen von Treibern zum Windows PE-Abbild

Wenn Ihre Geräte über Hardware verfügen, die nicht vom Windows PE-Standardabbild unterstützt wird, können Sie dem Abbild Treiber hinzufügen. Dieses Dialogfeld unterstützt zwei Treibertypen:

- OEM-Speichertreiber, die eine txtsetup.oem-Datei enthalten.
- Nicht-OEM-Speichertreiber, die eine .inf-Datei enthalten.

So fügen Sie dem Windows PE-Abbild zusätzliche Treiber hinzu

1. Klicken Sie im Bereich **Betriebssystembereitstellung** auf die Schaltfläche **Treiber im Windows PE-Abbild verwalten** in der Symbolleiste.
2. Steuern Sie zu der Windows PE-Abbilddatei, die Sie aktualisieren möchten.
3. Klicken Sie auf den Treibertyp, den Sie installieren möchten, und klicken Sie auf **Weiter**.
4. Klicken Sie auf **Hinzufügen** und navigieren Sie zur .inf- oder txtsetup.oem-Datei und den zugehörigen Dateien. Klicken Sie auf **Weiter**.
5. Geben Sie an, wie viel Platz im Windows PE-Abbild verfügbar sein soll, nachdem Sie die Größe des Abbilds geändert haben.
6. Klicken Sie abschließend auf **Weiter**.

Anpassen des Hintergrunds des Windows PE-Abbilds

Sie können den für ein Windows PE-Abbild verwendeten Hintergrund anpassen.

So ändern Sie den Hintergrund des Windows PE-Abbilds

1. Klicken Sie im Fensterausschnitt **Betriebssystembereitstellung** auf die Schaltfläche **Den Hintergrund des Windows PE-Abbilds ändern** in der Symbolleiste.
2. Wählen Sie aus, ob die Windows PE-Abbilddatei, die Sie verwenden möchten, auf 32-Bit- oder auf 63-Bit-Betriebssysteme angewendet werden soll.
3. Steuern Sie zu der Hintergrunddatei, die Sie verwenden möchten. Das beste Ergebnis erzielen Sie mit einer 24-Bit 800x600-Bitmap-Datei.
4. Klicken Sie abschließend auf **OK**.

Anhang: Zusätzliche Informationen zur Betriebssystembereitstellung und Profilmigration

Dieses Kapitel enthält zusätzliche Informationen zu den LANDesk Funktionen für die Betriebssystem-Abbilderstellung und Profilmigration.

Dieses Kapitel befasst sich mit folgenden Themen:

- "Erstellen einer Imaging-Bootdiskette" auf Seite 426
- "Hinzufügen von Anwendungspaketverteilungen an das Ende eines OSD-Skripts" auf Seite 427
- "Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten" auf Seite 427
- "Erstellen benutzerdefinierter Computernamen" auf Seite 428
- "Anpassen des Abschnitts [RunOnce] der Datei SYSPREP.INF durch Token-Inventarwerte." auf Seite 429
- "Verwenden von Abbildern in Umgebungen mit Einzel- und Multiprozessor-Systemen" auf Seite 429
- "Hinzufügen von Netzwerkadaptertreibern zur DOS-Bootumgebung" auf Seite 430
- "Hinzufügen von Netzwerkadaptertreibern zur Windows PE-Bootumgebung" auf Seite 432
- "Verwenden des LANDesk-Abbilderstellungstools für DOS" auf Seite 432
- "Verwenden des LANDesk-Abbilderstellungstools für Windows" auf Seite 435
- "Die Windows PE-Prebootumgebung" auf Seite 438

Erstellen einer Imaging-Bootdiskette

Die Funktion "Betriebssystembereitstellung" (OSD, Operating System Deployment) von LANDesk umfasst ein Dienstprogramm zum Erstellen von Bootdisketten, mit dem Sie mühelos eine Diskette erstellen können, um Geräte in Ihrem LANDesk Netzwerk in einen verwalteten Zustand hochzufahren. Sie können diese Bootdiskette einsetzen, um OSD-Aufträge auf Geräte fortzuführen, die kein Betriebssystem besitzen oder aus irgendeinem Grund einen Auftrag nicht ausführen konnten und sich jetzt nicht mehr starten lassen. Sobald Sie ein Gerät mit dieser Bootdiskette hochgefahren haben, können Sie einen Auftrag für dieses Gerät planen.

HINWEIS: Ein Benutzer muss zum Erstellen einer OSD-Bootdiskette über Administratorrechte auf dem Coreserver verfügen (selbst wenn er bereits über die OSD-Berechtigung verfügt).

Bootdisketten werden bei ihrer Erstellung mit dem Coreserver verknüpft. Falls Sie mehrere Coreserver einsetzen, verwenden Sie eine Bootdiskette, die von dem Coreserver erstellt wurde, an den das Gerät Daten senden soll.

So erstellen Sie eine Imaging-Bootdiskette

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie im Fenster **Betriebssystembereitstellung** in der Symbolleiste auf die Schaltfläche **Bootdiskette erstellen**, um das Dialogfeld "Imaging-Bootdiskette erstellen" zu öffnen.
3. Legen Sie eine 1,44-MB-Diskette in das Diskettenlaufwerk ein und stellen Sie sicher, dass das Zieldiskettenlaufwerk korrekt ist.

HINWEIS: Alle auf der Diskette vorhandenen Daten werden gelöscht.

4. Wählen Sie den Netzwerkadapter, der von dieser Bootdiskette unterstützt werden soll. Wegen des beschränkten Speicherplatzes unterstützt jede Diskette nur einen Adapter.
5. Klicken Sie auf **Start**. Im Statusfeld wird der Verlauf der Diskettenerstellung angezeigt.
6. Nach der Fertigstellung klicken Sie auf **Schließen**, um das Dialogfeld zu schließen.

Hinzufügen von Anwendungspaketverteilungen an das Ende eines OSD-Skripts

Sie können eine Enhanced Software Distribution- (ESWD)-Anwendungspaketverteilung problemlos zu einem Teil Ihres Betriebssystembereitstellungsskripts machen.

So fügen Sie ESWD-Pakete einem Betriebssystembereitstellungsskript hinzu

1. Öffnen Sie das Paketskript im Verzeichnis LANDesk/ManagementSuite/Scripts und kopieren Sie die REMEXECx=Zeilen für die Paketverteilung.
2. Bearbeiten Sie das Skript, indem Sie mit der rechten Maustaste in das Fenster "Skripte verwalten" klicken und dann auf **Erweiterte Bearbeitung** klicken.
3. Fügen Sie die ESW REMEXEC-Befehle am Ende des Skripts ein und ändern Sie die Nummerierung der REMEXEC-Befehle, sodass die Nummern fortlaufend sind.
4. Fügen Sie vor den eingefügten ESWD-Zeilen eine Zeile für den Befehl LDSLEEP ein, die wie im nachstehenden Beispiel aussehen sollte. Damit wird dem Betriebssystem Zeit gegeben, vor dem Beginn der Paketinstallation den Startvorgang zu beenden.

   ```
   REMEXECxx=LDSLEEP.EXE 120
   ```

   Ersetzen Sie xx durch eine eindeutige fortlaufende Nummer.

Verwenden von CSVIMPORT.EXE zum Importieren von Inventardaten

Zu LANDesk gehört ein Befehlszeilenprogramm, das den Import von Inventardaten in die Coredatenbank ermöglicht. Dies kann hilfreich sein, wenn Sie neue Geräte installieren und über Daten wie MAC-Adressen verfügen. Sie können diese Daten mit CSVIMPORT.EXE auf den Coreserver importieren, damit Sie Geräte frühzeitig als Ziel von Betriebssystembereitstellungsaufträgen angeben können.

CSVIMPORT.EXE benötigt eine Vorlagendatei, die den Inhalt der einzelnen Felder beschreibt und angibt, in welche Core-Datenbankspalten die betreffenden Daten geschrieben werden sollen. Zudem benötigt CSVIMPORT.EXE eine .CSV-Datei mit den Daten, die der von Ihnen angegebenen Vorlagendatei entsprechen. CSVIMPORT.EXE erstellt Miniscan-Dateien, die Sie in das Verzeichnis LANDesk/ManagementSuite/LDScan kopieren können, damit sie zur Coredatenbank hinzugefügt werden.

Beispiel für eine Vorlagendatei:

```
Network - NIC Address = %1%
 Network - TCPIP - Adapter 0 - Subnet Mask = 255.255.255.0
 BIOS - Serial Number = %2%
 BIOS - Asset Tag = %3%
 Display Name = %4%
```

Beachten Sie, dass Sie benutzerdefinierte Daten in die Dateien aufnehmen können. Die Einträge %1, %2 usw. beziehen sich auf die erste Spalte, die zweite Spalte und so weiter. In diesem Beispiel wird die Subnetzmaske 255.255.255.0 für alle Einträge übernommen. Die Spaltenüberschriften der Vorlagendatei müssen mit den tatsächlichen Feldnamen der Datenbank übereinstimmen; zusätzliche Informationen sind nicht zulässig.

.CSV-Beispieldatei:

```
0010A4F77BC3, SERIAL11, ASSETTAG-123-1, MACHINE1

 0010A4F77BC4, SERIAL21, ASSETTAG-123-2, MACHINE2

 0010A4F77BC5, SERIAL31, ASSETTAG-123-3, MACHINE3

 0010A4F77BC6, SERIAL41, ASSETTAG-123-4, MACHINE4

 0010A4F77BC7, SERIAL51, ASSETTAG-123-5, MACHINE5

 0010A4F77BC8, SERIAL61, ASSETTAG-123-6, MACHINE6
```

Rufen Sie CSVIMPORT mit den folgenden drei Parametern auf: <Vorlagendateiname> <csvDateiame> <AusgabeverzeichnisFürScandateien>. Wenn die Ausgabe sofort in die Coredatenbank eingetragen werden soll, geben Sie Ihr LANDesk/ManagementSuite/LDScan-Verzeichnis als Ausgabeverzeichnis an.

Erstellen benutzerdefinierter Computernamen

Auf der Seite **Benennungskonvention** des Assistenten für Tasks zur Betriebssystembereitstellung/Migration können Sie Computernamen definieren, die auf MAC-Adressen, auf von Ihnen eingegebenem Text und auf Zählern (nnn..) basieren. Außerdem können Sie Namen auf der Grundlage von Inventardaten für Assetkennzeichen, Seriennummern und Anmeldenamen erstellen, indem Sie eine Datei mit dem Namen COMPUTERNAME.INI anlegen.

COMPUTERNAME.INI-Syntax:

```
[Rename Operations]
tok0=ASSET TAG
tok1=SERIAL NUMBER
tok2=LOGIN NAME
```

Die von der .INI-Datei zurückgegebenen Werte ersetzen das $MAC-Token auf der Seite "Namenskonvention für Zielcomputer zuweisen" des Assistenten.

Sie können lediglich die drei oben genannten Inventarwerte in der Datei verwenden. Die Betriebssystem-Bereitstellung überprüft die Optionen in der Reihenfolge der tok<x>-Nummerierung. Die Datei muss nicht alle drei der oben genannten Token enthalten. Die erste tok<x>-Option, für die ein gleichbedeutender Datenbankeintrag gefunden wird, ersetzt den $MAC-Token für das abzubildende Gerät. Wenn beispielsweise die Datenbank im oben genannten Fall keine Einträge für Assetkennzeichen (ASSET TAG) oder Seriennummer (SERIAL NUMBER) enthält, aber ein Anmeldename (LOGIN NAME) verzeichnet ist, dann würde anstatt des $MAC-Tokens der Anmeldename verwendet. Stimmt keine der Optionen überein, wird die MAC-Adresse anstelle des $MAC-Tokens eingesetzt.

Die Anmeldenamensoption gibt den Anmeldenamen zurück, der vom letzten Inventarscan zurückgegeben wurde.

Verwenden des nnn-Tokens für Computernamen

Die Seite **Benennungskonvention** im Assistenten für Tasks zur Betriebssystembereitstellung/Migration enthält eine nnn-Option, die, abhängig von der Anzahl der angegebenen n, für eine 3- bis 15-stellige Zahl steht. Die Betriebssystembereitstellung verwaltet für jede Computernamensvorlage, die Sie im Assistenten angeben, einen fortlaufenden Zähler der verwendeten Nummern. So werden nachfolgende Aufträge dort fortgesetzt, wo der letzte Auftrag endete.

Jede eindeutige Vorlage besitzt einen eigenen Zähler. Wenn Sie immer dieselbe Vorlage verwenden, umfasst der Zähler verschiedene Aufträge. Falls Sie nach der Bereitstellung einiger Geräte die Vorlage ändern und später beschließen, wieder die ursprüngliche Vorlage zu verwenden, erinnert der Zähler, an welcher Nummer Sie für diese Vorlage mit dem Zählen aufgehört hatten, und setzt die Zählung fort.

Anpassen des Abschnitts [RunOnce] der Datei SYSPREP.INF durch Token-Inventarwerte.

Die Datei SYSPREP.INF enthält den Abschnitt [RunOnce], in dem Programme angegeben werden, die ausgeführt werden sollen, nachdem das Gerät zum ersten Mal gestartet wurde. Wenn Sie diesem Abschnitt eigene Programme hinzufügen, können Sie Datenbank-Token in die Programmbefehlszeile einfügen, falls sich dies für das auszuführende Programm empfiehlt. Die Betriebssystembereitstellung ersetzt die angegebenen Token durch die entsprechenden Core-Datenbankinformationen.

Beispieltoken:

```
%Computer - Device Name%
%Computer - Login Name%
%Computer - Manufacturer%
%Computer - Model%
%Computer - Type%
%Computer - BIOS - Asset Tag%
%Computer - BIOS - Service Tag%
%Network - TCPIP - Address%
%System - Manufacturer%
%System - Model%
%System - Serial Number%
%Processor - Processor Count%
%Computer - Workgroup%
%Computer - Domain Name%
```

Sie können mehrere Token miteinander verketten. Beispielsweise lassen sich zwei Token durch einen Doppelpunkt voneinander trennen: %Computer - Workgroup%:%Computer - Device Name% könnte "EigeneArbeitsgruppe:EigenerComputer" ergeben.

HINWEIS: Sie dürfen nur Token verwenden, die einen einzelnen Wert zurückgeben.

Verwenden von Abbildern in Umgebungen mit Einzel- und Multiprozessor-Systemen

Einzelprozessor- und Multiprozessorgeräte benötigen unterschiedliche Windows-Kernel. Je nach Hardwarekonfiguration können Sie möglicherweise ein für ein Einzelprozessorsystem erstelltes Abbild auch auf einem Multiprozessorgerät verwenden oder umgekehrt.

Geräte, die erweiterte Prozessorfunktionen unterstützen, verfügen in der Regel über einen Advanced Programmable Interrupt Controller (APIC). Geräte, die erweiterte Prozessorfunktionen unterstützen, können zudem mit einer Advanced Configuration and Power Interface (ACPI)-Schnittstelle ausgestattet sein.

Die Bedingungen, unter denen ein Abbild sowohl für Einzelprozessor- als auch Multiprozessorgeräte verwendet werden kann, sind kompliziert. Detaillierte Informationen hierzu finden Sie in der Datei UNATTEND.TXT von Microsoft. Im Allgemeinen müssen Sie Folgendes beachten, wenn Sie Abbilder für Einzelprozessor- und Multiprozessor-Systeme gemeinsam nutzen möchten:

HINWEIS: Sowohl die Quell- als auch die Zielgeräte müssen entweder über ein ACPI APIC HAL oder ein nicht-ACPI APIC HAL verfügen. Sie können auf einem APIC-Gerät ohne ACPI-Unterstützung kein ACPI-APIC-Abbild verwenden und umgekehrt auf einem ACPI-APIC-Gerät kein APIC-Abbild ohne ACPI-Unterstützung.

So konfigurieren Sie Multiprozessordaten

1. Wählen Sie auf der Seite **SysPrep-Optionen** des Assistenten für Tasks zur Betriebssystembereitstellung/Migration die Option **Erweiterte Multiprozessoroptionen konfigurieren**.
2. Wählen Sie auf der Seite **Multiprozessor** den Windows-Abbildtyp aus, den Sie bereitstellen.
3. Geben Sie an, ob das verwendete Abbild auf einem **Einzelprozessor**- oder **Multiprozessor**-Gerät erstellt wurde.
4. Ihre Quell- und Zielgeräte verfügen über dieselbe HAL. Falls das Abbild auf einem APIC-ACPI-Gerät erstellt wurde, wählen Sie **APIC**. Falls das Abbild auf einem APIC-ACPI-Gerät erstellt wurde, wählen Sie **MPS**.

Hinzufügen von Netzwerkadaptertreibern zur DOS-Bootumgebung

Eine Betriebssystembereitstellung durchläuft drei Phasen zur Netzwerkadaptertreibererkennung:

Stufe 1 (Windows):

NICINFO.EXE erkennt PnP-Treiber in Windows 2000/XP. Die Datei erkennt auch Windows 9x, wenn IE 4.02 oder höher installiert ist. NICINFO.EXE schreibt die erkannte Anbieter- und Gerätekennung in die Datei DOSNIC.INI des virtuellen Boot-Abbilds.

Stufe 2 (DOS)

AUTODETE.EXE sucht nach der von NICINFO.EXE hinterlassenen DOSNIC.INI-Datei und liest die Anbieter- und Gerätekennung. AUTODETE.EXE bezieht sich anschließend auf NIC.TXT, um den entsprechenden Treiber zu finden, der geladen werden soll. Das Programm kopiert den Treiber aus dem Verzeichnis c:\Net\Drivers des virtuellen Boot-Abbilds in das aktuelle RAM-Laufwerksabbild (Standardeinstellung r:\Net). AUTODETE.EXE trägt dann die entsprechenden Daten in die Microsoft-DOS-Konfigurationsdateien für den Netzwerkstapel (SYSTEM.INI und PROTOCOL.INI) ein.

Falls DOSNIC.INI leer ist, durchsucht AUTODETE.EXE alle PCI-Gerätesteckplätze nach Anbieter- und Gerätekennungen für Netzwerkadapter. Falls die gefundene Kennung einem Eintrag in der Datei NIC.TXT entspricht, lädt AUTODETE.EXE den betreffenden Treiber.

Stufe 3 (DOS)

Falls DOSNIC.INI leer ist und AUTODETE.EXE in der Datei NIC.TXT keinen Eintrag findet, der mit der erkannten Kennung übereinstimmt, wird der im Assistenten für Tasks zur Betriebssystembereitstellung/Migration angegebene Treiber geladen. Falls dieser Treiber nicht geladen wird, bleibt das Gerät in DOS hängen und muss von Ihnen manuell neu gestartet werden. Wenn im Assistenten kein Treiber angegeben wurde, legt AUTODETE.EXE eine Datei namens AUTODETE.LOG im Root-Verzeichnis des Laufwerks an und das Gerät wird wieder mit dem ursprünglichen Betriebssystem hochgefahren.

NICINFO.EXE und AUTODETE.EXE unterstützen keine 16-Bit-PCMCIA-Netzwerkadapter. Sie können Treiber für diese Netzwerkadapter laden, indem Sie, wie für Phase 3 beschrieben, im Assistenten für Tasks zur Betriebssystembereitstellung/Migration den entsprechenden Treiber auswählen. NICINFO.EXE kann Netzwerkadapter erkennen, die CardBus unterstützen.

NICINFO.EXE benötigt PnP-Unterstützung. Windows NT 4 unterstützt PnP-Geräte nicht.

Hinzufügen von Treibern für Netzwerkadapter

So fügen Sie Treiber für Netzwerkadapter hinzu

1. Bearbeiten Sie die Datei **ALTDRIVERS.INI** (im Verzeichnis \ManagementSuite\)
2. Bearbeiten Sie die Datei **NIC.TXT** im Verzeichnis ..\ManagementSuite\OSD\Utilities.
3. Verwenden Sie **COPYFILE.EXE**, um die .DOS- oder .EXE-Treiberdatei in das virtuelle Boot-Abbild unter **..\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG** einzufügen.
4. Fügen Sie die Datei **NIC.TXT** mithilfe von **COPYFILE.EXE** in das virtuelle Boot-Abbild ein.

Bearbeiten der Datei ALTDRIVERS.INI

ALTDRIVERS.INI ist die Treiberbeschreibungsdatei.

Beispieleintrag:

```
[Intel PRO/1000 Adapters]
DRIVER=E1000.DOS
PROTOCOL=E1000
```

- Zwischen den eckigen Klammern [ ] kann eine beliebige Beschreibung stehen. Diese Beschreibung wird im Assistenten für Tasks zur Betriebssystembereitstellung/Migration angezeigt, wenn Sie manuell einen Netzwerkadaptertreiber auswählen.
- DRIVER bezeichnet den .DOS- oder .EXE-Netzwerkadaptertreiber.
- PROTOCOL entspricht häufig dem Treibernamen oder dem Herstellernamen.

Bearbeiten der Datei NIC.TXT

Die Datei NIC.TXT enthält Informationen für die Erkennung von Netzwerkadaptern. Sie müssen die Datei NIC.TXT bearbeiten, wenn Sie benutzerdefinierte Adapterdaten hinzufügen möchten. Beispieleintrag:

```
ven=115D "Xircom"
dev=0003 "Xircom CardBus Ethernet 10/100 Adapter"
drv="CBENDIS.EXE"
prot="XIRCOM"
```

Vier Schlüssel und Werte können angegeben werden:

- **ven** umfasst vier Zeichen (zum Beispiel muss 1 in der Form 0001 angegeben werden); die Beschreibung ist beliebig.
- **dev** umfasst vier Zeichen; die Beschreibung ist beliebig.

- **drv** definiert den Treibernamen; als Standarderweiterung wird .DOS eingesetzt.
- **prot** gibt das Protokoll an, ist häufig mit dem Treibernamen oder dem Hersteller identisch.

Wie Sie der Datei NIC.TXT entnehmen können, sind nicht bei allen Treibern alle Schlüssel definiert.

Einfügen von Treiberänderungen in das virtuelle Boot-Abbild

Sie verwenden COPYFILE.EXE, um Treiberänderungen in das virtuelle Boot-Abbild einzufügen. Die Syntax lautet:

```
COPYFILE <Abbilddatei> <Quelldatei> <Zieldatei>
```

Beispiel:

```
COPYFILE c:\Programme\LANDesk\ManagementSuite\LANDesk\Vboot\LDVBOOT.IMG
c:\Drivers\MYNIC.DOS\Net\Drivers\MYNIC.DOS
```

HINWEIS: Für die Variable <Zieldatei> muss der Zielpfad ohne den Laufwerksbuchstaben angegeben werden.

Sie müssen den .DOS- oder .EXE-Netzwerkadaptertreiber in das Verzeichnis c:\Net\Drivers und die aktualisierte Datei NIC.TXT in das Verzeichnis C:\Net kopieren.

Hinzufügen von Netzwerkadaptertreibern zur Windows PE-Bootumgebung

Führen Sie die nachstehend beschriebenen Schritte aus, wenn Sie benutzerdefinierte Netzwerktreiber zu einer Windows PE-Umgebung hinzufügen möchten.

So fügen Sie Netzwerktreiber zur Windows PE-Bootumgebung hinzu

1. Kopieren Sie die .INF- und .SYS-Netzwerktreiberdateien in folgenden Ordner auf dem Coreserver:

   ..\ManagementSuite\LANDesk\Vboot\winpedrv

2. Fügen Sie die Netzwerktreiberinformationen dieser Datei auf dem Coreserver hinzu (weitere Informationen finden Sie in den Beispieleinträgen der Datei):

   ..\ManagementSuite\altdriverspe.ini

Verwenden des LANDesk-Abbilderstellungstools für DOS

HINWEIS: Wenn Ihre Lizenz die Betriebssystembereitstellungs- und Profilmigrationskomponente umfasst, werden automatisch Dateien für das LANDesk Abbilderstellungstool auf dem Coreserver installiert. Wenn Sie das LANDesk Abbilderstellungstool von einem anderen Speicherort ausführen möchten, müssen Sie die folgenden vier Dateien kopieren: IMAGEALL.EXE, IMAGE.EXE, RESTALL.BAT und BACKALL.BAT.

Das LANDesk-Abbilderstellungstool für DOS (IMAGE.EXE) ist ein DOS-basiertes Sicherungs- und Wiederherstellungsprogramm, das eine vollständige Statusaufnahme von einer Partition oder einem Datenträger erstellt und direkt auf die meisten ATAPI CD-R/RW-Laufwerke speichert. Sollte diese Partition oder dieser Datenträger jemals unbrauchbar werden, so können Sie ganz einfach das Abbild der Statusaufnahme wiederherstellen.

Beschränkungen

IMAGE.EXE ist für die Verarbeitung von Datenträgerfunktionen auf das BIOS angewiesen. Wenn das Computer-BIOS aus irgendwelchen Gründen den Zugriff auf die Festplatte limitiert und kein Drive Manager zur Verfügung steht, um diese Beschränkung zu korrigieren, dann ist auch IMAGE.EXE Beschränkungen unterworfen.

Systemanforderungen

- IBM-kompatibler Personal Computer mit einem i80386-kompatiblen Mikroprozessor oder besser
- 16 MB RAM
- XMS

Erste Schritte

IMAGEW.EXE wird als Teil der LANDesk-Betriebssystembereitstellung im Verzeichnis \Programme\LANDesk\ManagementSuite\osd\imaging installiert.

Umgebungsvariablen

IMAGE.EXE unterstützt die Verwendung mehrerer unterschiedlicher Umgebungsvariablen:

- **IMSG** blendet eine Meldung auf dem Bildschirm ein. Um mit IMSG eine Meldung zu erstellen, verwenden Sie den Befehl "set" (d. h., set imsg=<eine aus maximal 80 Zeichen bestehende Meldung hier hinzufügen>).
- **IBXT** ändert die Methode, mit der ein Satz CDs gebrannt wird, sodass IMAGE.EXE während einer Wiederherstellung nicht die letzte CD anfordert. Setzen Sie IBXT auf den Wert 1 (d. h., set ibxt=1). Diese Einstellung wird möglicherweise nicht von allen CD-R/RW-Laufwerken unterstützt.
- **IAR** ermöglicht es IMAGE.EXE, beim Schreiben eines Abbilds in eine Datei automatisch auf Benutzereingaben und Fehlermeldung zu reagieren. Setzen Sie IAR auf Y oder N (d. h., set iar=Y). Mit dieser Einstellung werden alle 'Y'es- oder 'N'o-Eingabeaufforderungen, die seitens des Benutzers eine Bestätigung mit der Eingabetaste erforderlich machen, automatisch beantwortet. Sie können DOS-Fehlerebenen in einer Stapeldatei verwenden, um festzustellen, ob der Vorgang erfolgreich war oder abgebrochen wurde.
- **IOBS=A** testet die Netzwerkgeschwindigkeit und verwendet die beste Puffergröße für den Upload/Download eines Abbilds.

Befehlszeilenoptionen

Sie können in Verbindung mit IMAGE.EXE Befehlszeilenoptionen verwenden. Trennen Sie die Optionen durch Leerschritte und geben Sie sie in der unten angezeigten Reihenfolge ein. Mit der Befehlszeilenoption /? können Sie eine Liste zusätzlicher Befehlszeilenoptionen anzeigen, die hier nicht erläutert werden.

So erstellen Sie ein komprimiertes Abbild in einer Datei

Format 1: image /Ch# d:\Dateiname.img (keine Validierung)

Format 2: image /Ch#V d:\Dateiname.img (Validierung)

Format 3: image /Ch#VB d:\Dateiname.img (Byte-für-Byte-Validierung)

Erläuterung: Ersetzen Sie "h" durch die Nummer 0 bis 7 der Quellfestplatte und "#" durch die Partitionseintrags-ID. Für die meisten Benutzer ist die Partitions-ID eine Zahl zwischen 1 und 4; für Datenträger ist sie eine Zahl, die als 0xPVV formatiert wurde, wobei P die erweiterte Partition und VV die Datenträgernummer im Hexadezimalformat von 01 bis FF ist.

Wenn Ihnen die Partitions- oder Datenträger-ID nicht bekannt ist, führen Sie IMAGE.EXE ohne jegliche Befehlszeilenoptionen aus und wählen Sie "Abbild erstellen". Der Bildschirm, in dem die Partitionen und Datenträger aufgelistet werden, zeigt die ID (in Klammern) als eine Hexadezimalzahl an. Sie sollten dieser Zahl ein 0x in der Befehlszeile voranstellen.

So erstellen Sie ein nicht komprimiertes Abbild in einer Datei

Format 1: image /Ch# /U d:\Dateiname.img (keine Validierung)

Format 2: image /Ch#V /U d:\Dateiname.img (Validierung)

Format 3: image /Ch#VB /U d:\Dateiname.img (Byte-für-Byte-Validierung)

Erläuterung: Wie oben.

So erstellen Sie ein komprimiertes Abbild in einem CD-Laufwerk

Format 1: image /Ch# /CDx (ATAPI)

Format 2: image /Ch# /CDSx (ASPI)

Erläuterung: Die Informationen bzgl. "h" und "#" sind dieselben wie weiter oben. Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x (/CD oder /CDS) aus, um eine Geräteliste zu erhalten.

So erstellen Sie ein nicht komprimiertes Abbild in einem CD-Laufwerk

Format 1: image /Ch# /U /CDx (ATAPI)

Format 2: image /Ch# /U /CDSx (ASPI)

Erläuterung: Wie oben.

So stellen Sie ein Abbild aus einer Datei wieder her

Format 1: image /R d:\Dateiname.img (keine Validierung)

Format 2: image /RV d:\Dateiname.img (Validierung nach Bedarf)

Erläuterung: Stellt das Abbild im selben Festplattenlaufwerk und im selben Speicherort wieder her, von dem aus das Abbild erstellt wurde.

So stellen Sie ein Abbild von einer CD wieder her

Format 1: image /R /CDx (ATAPI)

Format 2: image /R /CDSx (ASPI)

Erläuterung: Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x (/CD oder /CDS) aus, um eine Geräteliste zu erhalten.

So limitieren Sie die Dateigröße beim Erstellen

Format: d:\Dateiname;s

Erläuterung: Ersetzen Sie das "s" nach ";" durch 0 für 2 GB, 1 für 698 MB oder 2 für 648 MB.

Zur Beachtung

- Beim Erstellen eines Abbilds sollten Sie die Partition, von der die Sicherungskopie erstellt werden, nicht als Speicherort für die Abbilddatei verwenden. Falls Sie dies tun, wird die Partition zur selben Zeit aktualisiert wie versucht wird, eine Sicherungskopie von ihr zu erstellen. Dies hat zur Folge, dass sich

das Dateisystem beim Wiederherstellen der Partition in einem nicht synchronisierten Zustand befindet.

- Das Abbild sollte nicht auf der Partition wiederhergestellt werden, in der sich die Quelldatei für das Abbild befindet. Wenn Sie dies tun, überschreibt die Wiederherstellung die Dateisystemstrukturen und die eigentliche Abbilddatei.
- Nach der Wiederherstellung wird das System neu gestartet. Dies ist erforderlich, da die vom Betriebssystem verwendeten Partitionen und das Dateisystem sich geändert haben. Wird kein Neustart ausgeführt, so nimmt das Betriebssystem an, dass die Partition und das Dateisystem sich im selben Zustand befinden wie vor der Wiederherstellung. Dies kann Datenschäden verursachen. Sie können eine Befehlszeilenwiederherstellung mit /RN überschreiben. /RN sollte jedoch nur von versierten Benutzern verwendet werden, die wissen, dass die Nichtausführung des Neustarts kein Risiko darstellt.
- Beim Durchführen einer Befehlszeilenwiederherstellung wird die wiederhergestellte Partition auf dieselbe Festplattennummer und in dieselbe physikalische Speicherposition auf dem Laufwerk geschrieben, von der aus ihre Sicherungskopie erstellt wurde. Wenn dies ein Datenträger (Volume) war und es jetzt an dieser Speicherposition keine erweiterte Partition gibt, versucht die Wiederherstellung, die ursprüngliche erweiterte Partition zu erstellen. Wenn die erweiterte Partition nicht erstellt werden kann, wird sie als primäre Partition wiederhergestellt. Wenn die Position, von der aus die Partition gesichert wurde, eine primäre Partition war und dieser Stelle jetzt von einer erweiterten Partition belegt wird, wird sie als Datenträger (Volume) wiederhergestellt. Wenn eine vorhandene Partition oder ein Datenträger (Volume) an derselben Stelle beginnt wie die wiederherzustellende Partition, wird eine Warnmeldung eingeblendet, bevor die betreffende Partition oder das Volume überschrieben wird.
- Um den Wiederherstellungsprozess durch Starten der CD auszuführen, benötigen Sie ein ATAPI CD-Laufwerk. Für SCSI-Laufwerke müssen Sie Ihre eigene CDBOOT.F35-Datei erstellen, um die geeigneten DOS ASPI-Treiber zu laden und IMAGE.EXE nach Bedarf über AUTOEXEC.BAT zu starten.

Verwenden des LANDesk-Abbilderstellungstools für Windows

Das LANDesk Abbilderstellungstool für Windows (IMAGEW.EXE) ist ein Windows 32-basiertes Sicherungs- und Wiederherstellungsprogramm, das eine vollständige Statusaufnahme von einer Partition oder einem Datenträger erstellt und direkt auf die meisten DVD+RW oder CD-R/R-Laufwerke speichert. Sollte diese Partition oder dieser Datenträger jemals unbrauchbar werden, so können Sie ganz einfach das Abbild der Statusaufnahme wiederherstellen.

IMAGEW.EXE ist mit dem LANDesk Abbilderstellungstool für DOS (IMAGE.EXE) kompatibel.

Aktualisierte Version von IMAGEW

LANDesk Management Suite umfasst jetzt eine aktualisierte Version 2 von IMAGEW, die Unterstützung für Windows 7 bietet. Diese Version speichert Abbilddateien mit einer anderen Erweiterung und bietet einige neue Funktionen. Wenn Sie in der Vergangenheit die Version 1 von IMAGEW verwendet haben, können Sie diese Version weiterhin, wie im folgenden Abschnitt beschrieben, verwenden.

Version 2 von IMAGEW.EXE wird als Teil der LANDesk Betriebssystembereitstellung im Verzeichnis ..\ManagementSuite\osd\imagew 2 installiert.

Informationen zur Verwendung von IMAGEW 2 finden Sie auf der Website der LANDesk Support Community unter community.landesk.com.

Verwenden von IMAGEW Version 1

Die folgenden Informationen gelten für IMAGEW Version 1.

Beschränkungen

Für die Verwendung mit Windows 9x/Me setzt IMAGEW.EXE voraus, dass das System Int 13h-Erweiterungen unterstützt. Wenn Ihr Computer-BIOS aus irgendwelchen Gründen den Zugriff auf die Festplatte limitiert und kein Drive Manager zur Verfügung steht, um diese Beschränkung zu korrigieren, dann ist IMAGE.EXE auf diesen Betriebssystemen ebenfalls Beschränkungen unterworfen.

Systemanforderungen

- IBM-kompatibler Personal Computer mit einem i80386-kompatiblen Mikroprozessor oder besser
- Windows 32-basierte Umgebung mit mindestens 32 MB RAM wird empfohlen
- Administratorrechte bei der Ausführung unter Windows.

IMAGEW.EXE wird als Teil der LANDesk-Betriebssystembereitstellung im Verzeichnis \Programme\LANDesk\ManagementSuite\osd\imaging installiert.

Erstellen von Abbildern

Sie können unterschiedliche Umgebungsvariablen und Befehlszeilenoptionen verwenden, um sicherzustellen, dass die erstellten Abbilder Ihren Anforderungen genügen.

Umgebungsvariablen

Die Umgebungsvariablen für IMAGEW.EXE müssen mit Befehlszeilenoptionen verwendet werden. Folgende Umgebungsvariablen stehen zur Verfügung:

- **IBXT** ändert die Methode, mit der ein Satz CDs gebrannt wird, sodass IMAGEW.EXE während einer Wiederherstellung nicht die letzte CD anfordert. Setzen Sie IBXT auf den Wert 1 (d. h., set ibxt=1). Diese Einstellung wird möglicherweise nicht von allen CD-R/RW-Laufwerken unterstützt.
- **IAR** ermöglicht es IMAGEW.EXE, beim Schreiben eines Abbilds in eine Datei automatisch auf Benutzereingaben und Fehlermeldung zu reagieren. Setzen Sie IAR auf Y oder N (d. h., set iar=Y). Mit dieser Einstellung werden alle 'Y'es- oder 'N'o-Eingabeaufforderungen, die seitens des Benutzers eine Bestätigung mit der Eingabetaste erforderlich machen, automatisch beantwortet. Sie können DOS-Fehlerebenen in einer Stapeldatei verwenden, um festzustellen, ob der Vorgang erfolgreich war oder abgebrochen wurde.

Befehlszeilenoptionen

Sie können in Verbindung mit IMAGEW.EXE Befehlszeilenoptionen verwenden. Trennen Sie die Optionen durch Leerschritte und geben Sie sie in der unten angezeigten Reihenfolge ein. Mit der Befehlszeilenoption /? können Sie eine Liste von Befehlszeilenoptionen anzeigen, die hier nicht erläutert werden.

So erstellen Sie ein komprimiertes Abbild in einer Datei

Format 1: imagew /Ch# d:\Dateiname.img (keine Validierung)

Format 2: imagew /Ch#V d:\Dateiname.img (Validierung)

Format 3: imagew /Ch#VB d:\Dateiname.img (Byte-für-Byte-Validierung)

Erläuterung: Ersetzen Sie "h" durch die Nummer 0 bis 7 der Quellfestplatte und "#" durch die Partitionseintrags-ID. Für die meisten Benutzer ist die Partitions-ID eine Zahl zwischen 1 und 4; für Datenträger ist sie eine Zahl, die als 0xPVV formatiert wurde, wobei P die erweiterte Partition und VV die Datenträgernummer im Hexadezimalformat von 01 bis FF ist.

Wenn Ihnen die Partitions- oder Datenträger-ID nicht bekannt ist, führen Sie IMAGEW.EXE ohne jegliche Befehlszeilenoptionen aus und wählen Sie "Abbild erstellen". Der Bildschirm, in dem die Partitionen und Datenträger aufgelistet werden, zeigt auch die ID in Klammern als eine Hexadezimalzahl an. Sie sollten dieser Zahl ein 0x in der Befehlszeile voranstellen.

So erstellen Sie ein nicht komprimiertes Abbild in einer Datei

Format 1: imagew /Ch# /U d:\Dateiname.img (keine Validierung)

Format 2: imagew /Ch#V /U d:\Dateiname.img (Validierung)

Format 3: imagew /Ch#VB /U d:\Dateiname.img (Byte-für-Byte-Validierung)

Erläuterung: Wie oben.

So erstellen Sie ein komprimiertes Abbild in einem CD-Laufwerk

Format 1: imagew /Ch# /CDx

Erläuterung: Die Informationen bzgl. "h" und "#" sind dieselben wie weiter oben. Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x aus, um eine Geräteliste zu erhalten.

So erstellen Sie ein nicht komprimiertes Abbild in einem CD-Laufwerk

Format 1: imagew /Ch# /U /CDx

Erläuterung: Wie oben.

So stellen Sie ein Abbild aus einer Datei wieder her

Format 1: imagew /R d:\Dateiname.img (keine Validierung)

Format 2: imagew /RV d:\Dateiname.img (Validierung bei Bedarf)

Erläuterung: Stellt das Abbild im selben Festplattenlaufwerk und im selben Speicherort wieder her, von dem aus das Abbild erstellt wurde.

So stellen Sie ein Abbild von einer CD wieder her

Format 1: imagew /R /CDx

Erläuterung: Das x nach /CD entspricht der Nummer des zu verwendenden CD-Laufwerks. Lassen Sie das x aus, um eine Geräteliste zu erhalten.

So limitieren Sie die Dateigröße beim Erstellen

Format: d:\Dateiname;s

Erläuterung: Ersetzen Sie das "s" nach ";" durch 0 für 2 GB, 1 für 698 MB oder 2 für 648 MB.

Zur Beachtung

- Für die Ausführung unter Windows NT/2000/XP Pro werden Administratorrechte benötigt. Unter Windows 2000/XP wird die Ausführung als beliebiger Benutzer unterstützt. Klicken Sie hierfür mit der rechten Maustaste und wählen Sie die Option "Ausführen als".
- Beim Erstellen eines Abbilds sollten Sie die Partition, von der die Sicherungskopie erstellt werden, nicht als Speicherort für die Abbilddatei verwenden. Falls Sie dies tun, wird die Partition zur selben Zeit aktualisiert wie versucht wird, eine Sicherungskopie von ihr zu erstellen. Dies hat zur Folge, dass sich das Dateisystem beim Wiederherstellen der Partition in einem nicht synchronisierten Zustand befindet.

- Wenn Sie eine Sicherung durchführen, ohne eine Sperrung angefordert zu haben, befindet sich die Sicherung möglicherweise nicht in einem synchronisierten Zustand, wenn das Laufwerk während des Sicherungsvorgangs aktualisiert wurde.
- Das Abbild kann nicht auf der Partition wiederhergestellt werden, in der sich die Quelldatei für das Abbild befindet. Wenn Sie dies tun, überschreibt die Wiederherstellung die Dateisystemstrukturen und die eigentliche Abbilddatei.
- Nach der Wiederherstellung muss das System möglicherweise neu gestartet werden. Dies ist unter bestimmten Bedingungen erforderlich und wird durch das Programm bestimmt. Wenn Sie trotz Aufforderung keinen Neustart ausführen, nimmt das Betriebssystem an, dass die Partition und das Dateisystem sich im selben Zustand befinden wie vor der Wiederherstellung. Dies kann Datenschäden verursachen. Sie können eine Befehlszeilenwiederherstellung mit /RN überschreiben. /RN sollte jedoch nur von versierten Benutzern verwendet werden, die wissen, dass die Nichtausführung des Neustarts kein Risiko darstellt.
- Beim Durchführen einer Befehlszeilenwiederherstellung wird die wiederhergestellte Partition auf dieselbe Festplattennummer und in dieselbe physikalische Speicherposition auf dem Laufwerk geschrieben, von der aus ihre Sicherungskopie erstellt wurde. Wenn dies ein Datenträger (Volume) war und es jetzt an dieser Speicherposition keine erweiterte Partition gibt, versucht die Wiederherstellung, die ursprüngliche erweiterte Partition zu erstellen. Wenn die erweiterte Partition nicht erstellt werden kann, wird sie als primäre Partition wiederhergestellt. Wenn die Position, von der aus die Partition gesichert wurde, eine primäre Partition war und dieser Stelle jetzt von einer erweiterten Partition belegt wird, wird sie als Datenträger (Volume) wiederhergestellt. Wenn eine vorhandene Partition oder ein Datenträger (Volume) an derselben Stelle beginnt wie die wiederherzustellende Partition, wird eine Warnmeldung eingeblendet, bevor die betreffende Partition oder das Volume überschrieben wird.
- Um den Wiederherstellungsprozess durch Starten der CD auszuführen, benötigen Sie ein ATAPI CD-Laufwerk. Für SCSI-Laufwerke müssen Sie Ihre eigene CDBOOT.F35-Datei erstellen, um die geeigneten DOS ASPI-Treiber zu laden und IMAGEW.EXE nach Bedarf über AUTOEXEC.BAT zu starten.

Die Windows PE-Prebootumgebung

Windows PE ist ein Mini-Windows-System, das beschränkte Dienste basierend auf dem Window-Kernel bietet. Windows PE ist eine Hardware-unabhängige Windows-Umgebung, die folgendes beinhaltet:

- eine Untermenge der Microsoft Win32-Anwendungsprogrammierschnittstellen (APIs),
- einen Befehls-Interpreter, der Batchdateien ausführen kann,
- Unterstützung zum Hinzufügen von Windows Script Host (WSH), HTML-Anwendungen (HTA) und Microsoft ActiveX Data Objects (ADO), um benutzerdefinierte Tools oder Skripte zu erstellen.

Windows PE verwendet TCP/IP, um Netzwerkzugriff zu bieten und unterstützt denselben Satz von Netzwerk- und Massenspeichergerätetreibern, den auch Windows unterstützt. Es gibt einige bemerkenswerte Beschränkungen, z.B. dass die Konnektivität nur auf ausgehende Geräte beschränkt ist (Ressourcenfreigabe ist deaktiviert) und dass zur Verhinderung der Client-Nutzung des Betriebssystems nach 24 Std. Betrieb ein fest eingebauter Neustart stattfindet.

LANDesk hat das Windows PE-Betriebssystem so angepasst, dass es nur die notwendigen Bibliotheken, Dienstprogramme und Treiber enthält. Außerdem wurden die LANDesk-Agentendateien in das Abbild kopiert, um die LANDesk-Funktionalität zu vereinfachen. Die ursprünglich vom PE-Betriebssystem geladene Befehlszeile wurde auch geändert und enthält die LANDesk-Befehle zum Zurückspeichern. Ab Service-Pack 2 für LANDesk 8.7 wurde dem Abbild WMI-Support hinzugefügt.

In diesem Abschnitt finden Sie eine Liste der Dateien, die dem PE-Abbild entweder hinzugefügt oder geändert wurden, eine Übersicht des Bootverfahrens sowie eine Erklärung jeder Zeile in der Startbefehlsdatei.

Geänderte oder hinzugefügte Dateien im WinPE-Abbild

Außer den Treibern enthält das LANDesk Windows PE-Abbild folgende geänderte oder hinzugefügte Dateien:

Datei	Zweck
winbom.ini	Deaktiviert die Windows PE-Firewall
\i386\txtsetup.sif	LANDesk Signaturdatei
\i386\system32\winpeshl.ini	Definiert den Shell-Speicherort
\i386\system32\peshell.exe	Die tatsächlich verwendete Shell
\i386\system32\setupreg.hiv	Enthält den LANDesk Pfad
\i386\system32\startnet.cmd	Beim Start ausgeführte Befehlszeile
\i386\system32\all.reg	LANDesk Registrierungsänderungen
\i386\system32\winpe.bmp	LANDesk Hintergrundbild
\CBA8	LANDesk Agent
\LDCLIENT	LANDesk Agent

LANDesk WinPE-Bootprozess

Der WinPE-Bootprozess startet wie folgt:

1. Sobald der Bootsektor geladen ist, verwendet SETUPLDR zum Scannen der Hardware NTDETECT.COM, damit die richtige HAL geladen werden kann.
2. WINPEOEM.SIF wird zum Laden des Boottreibers verwendet (Administratoren können diese Datei anpassen, um zu steuern, welche Massenspeichertreiber geladen werden) und NTOSKRNL.EXE beendet dann das Umgebungssetup und ruft SMSS auf, das seinerseits die Registrierung lädt und Winlogon aufruft.
3. Winlogon startet die Dienste, beendet das Laden der Treiber und startet eine Benutzersitzung.
4. CMD.EXE wird ausgeführt und verarbeitet STARTNET.CMD. Diese Batchdatei wird zum Laden der Netzwerktreiber und alle anderen Befehle verwendet, die man hinzufügt. Die Windows PE STARTNET.CMD-Originaldatei sieht so aus:

   ```
   factory winpe
   ```

Das von LANDesk geänderte WinPE-Abbild enthält eine benutzerdefinierte STARTNET.CMD-Datei. In Version 8.7sp2 sieht diese folgendermaßen aus:

```
@echo off
```

```
set path=%path%;x:\cba8;x:\ldclient
\ldclient\GetBootOptions set /a err = %errorlevel%
if %err% gtr 0 goto nofix
ldclient\Diskinfo fix
:nofix
factory winpe
reg import all.reg
\ldclient\wait4ip /t 180
if %errorlevel% gtr 0 goto fail
CD \CBA8
RESIDENTAGENT.EXE /register
RESIDENTAGENT.EXE /start
CD \ldclient
winpepds /install
winpepds /start
If %err% gtr 0 goto pxe
miniscan /nodeviceid /usemacasname
Goto end
:pxe
if %err% lss 2 goto pxemenu
:pxeboot
miniscan /x /nodeviceid /usemacasname
goto end
:pxemenu
miniscan /nodeviceid /usemacasname
Replcore PxeMenuStart.cmd
call PxeMenuStart.cmd
goto end
:fail
@echo "Die IP-Adresse von "Localhost" konnte nicht ermittelt werden oder der Coreserver-Name konnte
nicht gelöst werden. Bitte prüfen Sie Netzwerk und versuchen Sie es nochmal."
@pause
:end
```

STARTNET.CMD Befehlsdefinitionen

Der folgende Abschnitt beschreibt jede Zeile in STARTNET.CMD.

@echo off

Blendet die Ausgabe dieser CMD-Datei aus. ENTF diesen Befehl bei der Fehlerbehebung der STARTNET.CMD.

set path=%path%;x:\cba8;x:\ldclient

Richtet den Pfad ein, damit er die hinzugefügten LANDesk Agentendateien enthält.

\ldclient\GetBootOptions

Diese ausführbare Datei legt die Fehlerebene auf 0, 1 oder 2 fest. Die Werte sind 0, wenn das Gerät virtuell gebootet wurde, 1, wenn das Gerät PXE-gebootet wurde und das PXE-Menü ausgewählt wurde und 2, wenn es PXE-gebootet wurde und verwaltetes Booten ausgewählt wurde.

set /a err = %errorlevel%

Legt die ERR-Variable für den von GetBootOptions ermittelten Wert fest.

if %err% gtr 0 goto nofix

Diese Zeile enthält das Skript "zur nächsten Zeile springen", wenn das Gerät PXE-gebootet wurde.

\ldclient\Diskinfo fix

Diese Zeile wird nur verarbeitet, wenn kein PXE-Boot durchgeführt wurde. Diskinfo.exe mit dem Reparatur-Switch setzt MBR zurück, damit es in die aktive Originalpartition zurückgebootet wird. Vbooting stellte dies zuvor zum Booten in das WinPE RAM-Laufwerk ein.

factory –winpe

Der Befehl FACTORY.EXE wird verwendet, um Treiber zu laden, und wenn sie vom –winpe-Switch aufgerufen wird, generiert sie einen eindeutigen Namen für die PE-Sitzung (normalerweise minint-<Zufallssuffix>) und verarbeitet dann die WINBOM.INI, die dort gespeichert ist, wo Sie das PE-Verhalten konfigurieren und hinzufügen können. Beispiel: Weil FACTORY.EXE standardmäßig alle verfügbaren Treiber scant, um denjenigen zu finden, der zu der erkannten Hardware passt, könnten Sie die Anzahl der gescannten Treiber limitieren (und dadurch die Boot-Geschwindigkeit hochsetzen), indem Sie den Abschnitt NetCards der WINBOM.INI-Datei ändern.

reg import all.reg

Importiert die Einstellungen der LANDesk-Einstellungen in der WinPE-Registrierung. Speziell der Name des Coreservers und der Anschluss, der für das Inventar verwendet wird, werden alle in der Datei ALL.REG definiert. Hier ein Beispiel für ALL.REG:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Intel\LANDesk\LDWM]
"CoreServer"="<core_name>"
"InventoryServerPort"="5007"
```

\ldclient\wait4ip /t 180

Die Ausführungsdatei wait4ip gewährleistet, dass wir eine IP-Adresse haben, bevor wir das Inventar dieses Geräts sammeln. /t 180 definiert einen Zeitablauf von 3 Minuten. Sie können ein /s hinzufügen, damit die Ausgabe dieses Programms im Hintergrund abläuft. Zusätzliche Informationen finden Sie, wenn Sie es mit /? ausführen.

if %errorlevel% gtr 0 goto fail

Überspringt den Rest der Befehle in dieser Datei, wenn keine IP-Adresse ermittelt werden kann.

CD \CBA8

Ändert das Verzeichnis von X:\i386\system32 in X:\CBA8.

residentagent.exe /register

RESIDENTAGENT.EXE ist der Dienst, der Verbindungen auf Remotebefehle abhört und diese akzeptiert und dann die entsprechende, benötigte Anwendung zur Verarbeitung des Antrags startet (so werden LANDesk-Abbildoperationen durchgeführt). Der /register-Switch installiert und registriert RESIDENTAGENT.EXE als einen Dienst. Dies wird im Verzeichnis CBA8 unter RESIDENTAGENT.LOG protokolliert.

residentagent.exe /start

Der /start-Switch startet den Dienst RESIDENTAGENT.EXE, der mit dem Laden der nötigen Bibliotheken fortfährt. Auch das wird unter RESIDENTAGENT.LOG protokolliert.

CD \LDClient

Ändert das Verzeichnis von X:\CBA8 in X:\LDClient.

winpepds /install

WINPEPDS ist das Modul, das der Coreserver anpingt, um dieses Gerät zu erkennen und dies als den richtigen verwalteten Knoten zu verifizieren. Der /install-Switch installiert den Dienst.

winpepds /start

Der /start-Switch installiert den WINPEPDS-Dienst.

if %err% gtr 0 goto pxe

Diese Zeile bedeutet, dass PXE-gebootete Geräte das Skript im Abschnitt PXE unten fortführen.

miniscan /nodeviceid /usemacasname

Diese Zeile wird nur bei virtuell gebooteten Geräten als letzter Befehl ausgeführt. Miniscan ist das Dienstprogramm, das zum Erfassen minimaler Informationen über das System verwendet wird und diese in der LDMS-Inventardatenbank speichert. Wenn Sie Miniscan ohne Switches ausführen, wird ein Gerätename und die Kennung in der Scandatei aufgenommen, die dann in der Konsole als "minint-<Zufallssuffix>" erscheinen. Wenn Sie jedoch die /nodeviceid /usemacasname-Switches verwenden, werden diese Informationen aus der Scandatei entfernt und die gesendeten Daten auf drei Dinge limitiert: MAC-Adressen, IP-Adressen und Prozessoranzahl. Auf der Konsole erscheinen diese Geräte unter dem Namen ihrer MAC-Adressen.

if %err% lss 2 goto pxemenu

Erkennt PXE-gebootete Geräte, die das Menü dazu bringen sollen, auf den Abschnitt PXEmenu zu springen.

miniscan /x /nodeviceid /usemacasname

Diese Zeile wird von den PXE-gebooteten Geräten ausgeführt, die verwaltet gebootet werden. Wenn /x zum Aufrufen eines Miniscans verwendet wird, wird ein zusätzliches Attribut im Netzwerkabschnitt der Scandatei gesendet: Pxeboot=ja.

miniscan /nodeviceid /usemacasname

Diese Zeile wird nur von PXE-gebooteten Geräten ausgeführt, die ein Menü anzeigen sollen. Miniscan ist das Dienstprogramm, das zum Erfassen minimaler Informationen über das System verwendet wird und diese in der LDMS-Inventardatenbank speichert. Wenn Sie Miniscan ohne Switches ausführen, wird ein Gerätename und die Kennung in der Scandatei aufgenommen, die dann in der Konsole als "minint-<Zufallssuffix>" erscheinen. Wenn Sie jedoch die /nodeviceid /usemacasname-Switches verwenden, werden diese Informationen aus der Scandatei entfernt und die gesendeten Daten auf drei Dinge limitiert: MAC-Adressen, IP-Adressen und Prozessoranzahl. Auf der Konsole erscheinen diese Geräte unter dem Namen ihrer MAC-Adressen.

replCore PxeMenuStart.cmd

Mit REPLCORE.EXE wird die %CoreServer%-Variable in der Datei, auf die es gerichtet ist, durch den Wert ersetzt, der im Wert der Registrierungszeichenfolge HKLM\Software\Intel\LANDesk\LDWM\CoreServer ermittelt wurde (diese wurde zuvor im Prozess mit ALL.REG bestückt). In diesem Fall wird gleich PxeMenuStart.cmd aufgerufen und verwendet sdclient zum Kontakt mit dem Coreserver und muss daher den richtigen Core Namen in seiner Befehlszeile enthalten.

call PxeMenuStart.cmd

Wenn die Menüoption vom PXE-gebooteten Gerät ausgewählt wurde, dann wird PXEMENUSTART.CMD ausgeführt. Die beiden maßgeblichen Zeilen sind:

```
sdclient /f /o /p="http://%CoreServer%/landesk/files/dosmenu.cfg"
```

```
RunBatch 500 X:\LDClient PxeMenu dosmenu.cfg
```

Zuerst wir sdclient zum Abrufen von DOSMENU.CFG vom Coreserver verwendet. Dann wird RunBatch (ein einfaches Dienstprogramm, das einen Prozess nach einer definierten Verzögerung aufruft) zum Starten von PXEMENU.EXE (mit dem Parameter von DOSMENU.CFG eingerichtet) verwendet.

@echo "Die IP-Adresse von "Localhost" konnte nicht ermittelt werden oder der Coreserver-Name konnte nicht gelöst werden. Bitte prüfen Sie Netzwerk und versuchen Sie es nochmal."

Wenn keine IP-Adresse erhalten wurde, erscheint diese Fehlermeldung. Sie gibt an, dass NIC oder die NIC-Treiber untersucht werden sollten.

Versorgung (Provisioning)

Versorgung – Übersicht

LANDesk "Versorgung" bietet Ihnen die Möglichkeit, alle Attribute und Funktionen Ihrer neuen Geräte zu definieren, bevor diese in Ihrer Umgebung eingeführt werden. Die Versorgung überträgt diese Attribut- und Funktionsgruppe mit einem automatisierten Verfahren auf die Geräte. Mit der Versorgung (auch als "Provisioning" bezeichnet) können Sie Ausfallzeiten vermindern und sicherstellen, dass neue Geräte zuverlässig und vorhersehbar arbeiten, wenn sie Teil Ihrer Produktionsumgebung werden. Sie können auf den Versorgungsverlauf eines jeden Geräts zugreifen, um herauszufinden, wann und was bereitgestellt wurde und es ggf. auf einen vorigen Zustand zurückzusetzen. Die Versorgung kann sowohl unter Windows als auch unter Linux ausgeführt werden. Vorlagen für beide Betriebssysteme werden auf die gleiche Weise erstellt.

Die Versorgung besteht aus einer Reihe von Aktionen, die auf einem Zielgerät auszuführen sind. *Aktionen* bilden die Grundeinheiten der Versorgung. Eine *Vorlage* besteht aus einer Sammlung von Aktionen, die in einer vordefinierten Abfolge ausgeführt werden. LANDesk stellt mehrere vorgefertigte Versorgungsvorlagen bereit, um Ihnen den Einstieg zu erleichtern. Diese Vorlagen sind für bestimmte Hardwarekonfigurationen optimiert, wie beispielsweise für Konfigurationen von Dell und Hewlett-Packard. Sie können diese Versorgungsvorlagen mit Ihren eigenen Hauptvorlagen kombinieren oder sie mit geringen Änderungen ausführen, um ein bestimmtes Dell- oder HP-Markengerät generisch zu versorgen. Sie können die Versorgungstasks auf dieselbe Weise aufteilen, wie die Arbeit beim manuellen Einrichten eines Systems.

Die Versorgung funktioniert auf neuen und auf dynamischen Geräten gleich gut. Sie können neue Geräte mit der exakten Konfiguration versorgen, die Sie benötigen, und die Konfiguration sogar schon vor dem Eintreffen des neuen Geräts einrichten. Sie können die Versorgung dazu verwenden, ein Gerät von einem Verwendungszweck auf einen anderen umkonfigurieren, indem Sie die Grundfunktionen dahingehend ändern, dass sie den sich wandelnden Anforderungen Ihrer Organisation gerecht werden.

Mithilfe der Alarmfunktionen können Sie sich benachrichtigen lassen, wenn Versorgungsereignisse stattfinden.

Versorgungsagent

Im Zentrum der Versorgungskomponente steht der Agent "ldprovision" im Ordner "/ldlogon/provisioning". Dieser Agent enthält kleine Anwendungen für jede Aktion. Der Agent befindet sich auf dem Zielgerät. Er wird über einen PXE-Server oder ein physikalisches Bootmedium, z. B. ein USB-Laufwerk oder eine CD, bereitgestellt.

Im Verlauf des Versorgungsprozesses durchläuft der Agent folgende Phasen:

- Er fordert die Konfigurationseinstellungen einer Vorlage von einem Webdienst auf dem Coreserver an.
- Er prüft das Kennzeichen für den Prebootumgebungstyp, um sicherzustellen, dass er in der richtigen Prebootumgebung ausgeführt wird.
- Er führt die Aktionen in der in der Konfiguration vorgegebenen Reihenfolge aus.
- Er startet das Gerät (bei Bedarf) neu.
- Er injiziert eine Version von sich selbst in das Zielbetriebssystem, damit er seine Arbeit fortsetzen kann, nachdem das echte Betriebssystem im Anschluss an den Neustart geladen wird.
- Er sendet Feedback an den Webdienst auf dem Core.

Der Agent führt alle erforderlichen Neustarts aus und geht unmittelbar nach jedem Neustart zur nächsten Aktion über. Die meisten Versorgungsaufgaben können vor der Inbetriebnahme eines neuen Geräts ausgeführt werden. Sie können eine Vorlage erstellen und den Task erstellen, der von der Vorlage auf dem neuen Gerät ausgeführt werden soll. Der Task wird erst bei der Ausführung des Versorgungsagenten auf dem neuen Gerät ausgeführt.

Um die Versorgungsfunktionalität vollständig nutzen zu können, benötigt der Benutzer die beiden folgenden Rechte: das Recht "Versorgung - Planen" und das Recht "Versorgung - Konfiguration". Mit diesen Rechten können Benutzer Versorgungsvorlagen erstellen, ändern und planen. Diese Rechte werden automatisch für jeden Benutzer mit Administratorrechten aktiviert; jedoch können sie bei Bedarf für jeden Benutzer aktiviert werden.

Preboot-Tools

Damit Versorgungstasks ausgeführt werden können, muss die Möglichkeit gegeben sein, das Gerät zu booten, bevor ein Betriebssystem darauf installiert wird. Dies lässt sich mit einem PXE-Server oder ein physisches Bootmedium (CD- oder USB-Laufwerk) erreichen. PXE ist die einfachste Möglichkeit, viele Computer gleichzeitig in derselben Prebootumgebung zu booten. CD- oder USB-Laufwerke sind portierbar und gewährleisten, dass der Computer, auf dem die Prebootumgebung ausgeführt wird, dem vom Administrator zu versorgenden Computer entspricht.

Die Prebootumgebung (PE, Preboot Environment) besteht aus einem Betriebssystem, das über Video- und Netzwerkfunktionen, einen kleinen Inventarscanner sowie über einen Agenten verfügt, der Dateien empfangen und Befehle ausführen kann. Dieser Agent führt ein Abbilderstellungstool oder skriptgesteuertes Installationstool zur Installation des Betriebssystems auf dem Gerät aus. Der Agent leitet den Versorgungsprozess ein. Die Versorgungskomponente unterstützt die Windows-Prebootumgebungen.

Sie benötigen keine separaten Bootmedien für jedes Clientsystem, da die Bootmedien für andere Geräte wiederverwendet werden können.

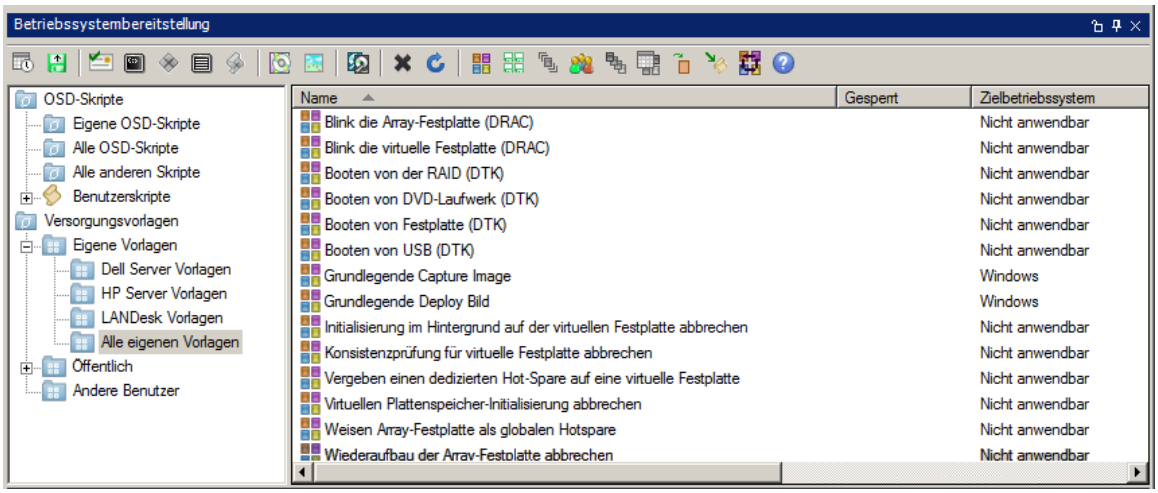
Unterschiede zwischen Betriebssystembereitstellung und Versorgung

Die Versorgungskomponente hat einen größeren Einsatzbereich als die Betriebssystembereitstellung. Während die Betriebssystembereitstellung Teil des Versorgungsprozesses sein kann, deckt sie jedoch nur einen Teil der Versorgung ab. Dagegen erstreckt sich die Versorgung über den gesamten Prozess des Vorbereitens eines Geräts für den sicheren Einsatz in Ihrer Umgebung – vom Anfang bis zum Ende. Die Tabelle unten verdeutlicht, wie sich die Versorgung von der Betriebssystembereitstellung unterscheidet.

Betriebssystembereitstellung	Versorgung (Provisioning)
Coregesteuert	Zielgerätgesteuert
Die Arbeit beginnt nach der Lieferung des Geräts.	Die meisten Aufgaben können vor der Lieferung des Geräts durchgeführt werden.
Erstreckt sich nur auf den Betriebssystembereitstellungsschritt der Versorgung.	Erstreckt sich über den gesamten Konfigurationsvorgang des Geräts – vom Anfang bis zum Ende.
Erfordert ein vollständiges Abbild, das nicht in Abschnitte zerlegt werden kann.	Besteht aus kleineren Vorlagen, die bearbeitet oder auf der Ebene der Vorlage ausgetauscht werden können.

Die Benutzeroberfläche der Versorgungskomponente

Die Extras der Versorgung sind Teil des Extras zur Betriebssystembereitstellung. (Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.) Versorgungsvorlagen werden in einer Strukturansicht angezeigt, und eine Symbolleiste gewährt Zugriff auf Dialogfelder zu verschiedenen Tasks.



In der Baumstruktur sind die verfügbaren Vorlagen in den folgenden Ordnern organisiert:

- **Eigene Vorlagen:** Von Ihnen erstellte Vorlagen. Nur Sie selbst und administrative Benutzer haben Zugriff auf diese Vorlagen.
- **Öffentlich:** Sowohl Ihre eigenen Vorlagen als auch als öffentlich gekennzeichnete Vorlagen.
- **Andere Benutzer** (nur administrative Benutzer): Eine Liste mit Benutzern und deren Vorlagen.

Öffentliche Vorlagen werden von Benutzern mit Administratorrechten erstellt und können von allen Benutzern angezeigt werden. Vorlagen im Ordner "Eigene Vorlagen" können von anderen Benutzern angezeigt, jedoch nur vom Ersteller der Vorlage oder von Benutzern mit Administratorrechten bearbeitet werden. Jedes Mal, wenn Sie eine nicht als "öffentlich" gekennzeichnete Vorlage verwenden, wird die Instanz der Vorlage gesperrt. Diese Instanz kann ausgeblendet, jedoch nicht gelöscht werden.

Im rechten Bereich werden die Vorlagen des markierten Ordners angezeigt, wobei die Vorlageneigenschaften in fünf Spalten erscheinen. Doppelklicken Sie auf eine Vorlage, um die zugehörigen Eigenschaften anzuzeigen, einschließlich einer Liste mit anderen Vorlagen, in denen die ausgewählte Vorlage enthalten ist.

Die Symbolleiste umfasst Schaltflächen zum Erstellen, Ändern und Verwalten von Versorgungsvorlagen.

- **Neue Versorgungsvorlage**: Dient der Erstellung einer neue Versorgungsvorlage.
- **Versorgungs-Bootmedien erstellen:** Zum Konfigurieren und Erstellen von Bootmedien.
- **Vorlage komprimieren**: Kombiniert alle eingeschlossenen Vorlagen in die ausgewählte Vorlage, so dass nur noch eine Vorlagendatei ausgeführt werden muss.
- **Öffentliche Variablen:** Hiermit können Sie globale Variablen, die für alle Versorgungsvorlagen gelten, anzeigen und festlegen.
- **Vorlagengruppe erstellen**: Hiermit können Sie Vorlagen organisieren, indem Sie Gruppen innerhalb eines Ordners erstellen.

- **Vorlage planen:** Öffnet das Extra "Geplante Tasks", in dem Sie Versorgungstasks und andere Verwaltungstasks einsehen können. Sie können Versorgungstasks planen und den Status von Tasks anzeigen.
- **Vorlagen importieren:** Importiert eine Vorlage in die Coredatenbank.
- **Installationsskripte:** Hiermit können Sie Installationsskripte zur Verwendung beim Erstellen skriptgesteuerter Installationsaktionen und zum Bereitstellen von Abbildaktionen in Vorlagen zur Verfügung stellen.
- **Vorlagen aktualisieren:** Hiermit können Sie Vorlagen von LANDesk downloaden und importieren sowie den Speicherort für den Vorlagendownload und die Proxyservereinstellungen konfigurieren.

Wenn Sie auf eine Vorlage doppelklicken, wird die Vorlagenansicht geöffnet. In dieser Ansicht können Sie die Aktionsliste ändern (Aktionen hinzufügen oder löschen, die Aktionsreihenfolge ändern usw.). Sie können Variablen ändern, die speziell für diese Vorlage gelten, die Liste der von dieser Vorlage einbezogenen Vorlagen oder die Liste der Vorlagen, in denen die Vorlage enthalten ist, anzeigen und ändern. Sie können Vorlagen veröffentlichen, ihren Verlauf anzeigen (falls die Vorlage ausgeführt wurde) und den XML-Code von Vorlagen anzeigen oder ändern.

Erstellung und Bearbeiten von Versorgungsvorlagen

Die Schaltfläche **Neue Vorlage** ist der Ausgangspunkt für die Erstellung einer neuen Vorlage. Wenn Sie eine Vorlage ändern möchten, klicken Sie mit der rechten Maustaste auf die Vorlage und wählen dann **Bearbeiten**. Um eine Vorlage zu entfernen, wählen Sie sie aus und klicken auf die Schaltfläche **Löschen**. Sie können nur Vorlagen löschen, die nie benutzt wurden.

Erstellen von Vorlagengruppen

Mithilfe von Versorgungsgruppen können Sie Ihre Vorlagen Ihren Anforderungen entsprechend organisieren. Sie können beispielsweise Gruppen auf der Basis spezifischer Anbieter und Untergruppen auf der Basis von Gerätemodellen erstellen. Untergruppen lassen sich bis zu sechs Ebenen tief schachteln.

Duplizieren vorhandener Vorlagen

Nachdem eine Vorlage benutzt wurde, kann sie nicht mehr direkt bearbeitet werden. Sie kann jedoch dupliziert und dann bearbeitet werden. Aus diesem Grund sollten Vorlagen ihrer Beschaffenheit nach nicht zu groß sein, damit Sie nur diese spezifische Komponente der Versorgungskonfiguration ändern müssen, falls Änderungen erforderlich werden.

Mit der Schaltfläche **Duplizieren** können Sie eine Kopie der ausgewählten Vorlage erstellen. Sie können die Kopie modifizieren, wobei Sie kleine Änderungen an der Kopie vornehmen, anstatt viel mehr Zeit in die Erstellung eine ganz neuen Vorlage zu investieren.

Wenn Sie eine öffentliche Vorlage duplizieren, wird die Kopie in den Ordner "Eigene Vorlagen" eingefügt und übernimmt die Eigenschaften einer privaten Vorlage.

1. Klicken Sie auf den Ordner **Öffentlich** oder den Ordner **Eigene Vorlagen**, um Vorlagen im rechten Fensterausschnitt anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf eine Vorlage und wählen Sie dann **Duplizieren** aus.

   Die Vorlage wird unter Verwendung des Namens der Originalvorlage und des Datums und der Uhrzeit der Duplikaterstellung in dem Ordner kopiert.

3. Um den Namen, die Beschreibung, Bootumgebung oder das Zielbetriebssystem der duplizierten Vorlage zu ändern, klicken Sie mit der rechten Maustaste auf das Duplikat, klicken auf **Eigenschaften**, ändern die Einstellungen und klicken auf **OK**.
4. Um die Aktionen, enthaltenen Vorlagen, Benutzervariablen oder den XML-Code der duplizierten Vorlage zu ändern, doppelklicken Sie auf das Duplikat, um die Ansicht **Vorlage** zu öffnen.

Komprimieren einer Vorlage

Mit der Schaltfläche **Komprimieren** können Sie verschiedene Vorlagen in einer Vorlage zusammenfassen. Wenn andere Vorlagen in der aktuellen Vorlage enthalten sind, wird deren XML-Code innerhalb des XML-Codes der Vorlage gespeichert, wodurch eine einzige XML-Datei entsteht. Nachdem Sie eine Vorlage komprimiert haben, lässt sie sich nicht mehr erweitern und wieder in einzelne Vorlagen zerlegen.

Schritte für die Versorgung eines Geräts

Die Versorgung eines Geräts ist im Wesentlichen ein aus drei Schritten bestehender Prozess. Zuerst erstellen Sie eine Versorgungsvorlage, konfigurieren die Vorlage mit den auf das Gerät zu übertragenden Elementen und planen dann einen Task, um die Vorlage auf dem Gerät auszuführen. Diese Schritte werden hier nur kurz beschrieben. Ausführliche Anweisungen finden sich in den nachfolgenden Abschnitten.

Schritt 1: Erstellen einer Vorlage

Um ein Gerät zu versorgen, erstellen Sie eine Vorlage. Eine Vorlage ist ein XML-Dokument, das mehrere Bausteine umfasst, die auf das Gerät angewendet werden. Die Bausteine bauen aufeinander auf und können aus Aktionen, Attributen, Beschränkungen usw. bestehen. Eine Vorlage kann eine oder eine Vielzahl von Aktionen umfassen.

Vorlagen können in einem Versorgungstask in einer bestimmten Reihenfolge miteinander verkettet werden. Die Taskreihenfolge in einer Vorlage kann geändert werden. Die Abfolge kann geändert werden, sofern dies sinnvoll ist (Sie können beispielsweise keinen Task, der nach der Installation des Betriebssystems auszuführen ist, vor einen Task setzen, der vor der Installation des Betriebssystems ausgeführt wird). Es gibt mehrere vorkonfigurierte Vorlagen für unterschiedliche Anbieter (HP, Dell usw.).

Vorlagen werden als XML-Dokumente in der Datenbank gespeichert.

Schritt 2: Konfigurieren der Vorlage

Nachdem Sie die Vorlage erstellt haben, müssen Sie sie konfigurieren, indem Sie ihr Aktionen hinzufügen. Vorlagenaktionen sind in fünf Abschnitte unterteilt. Sie können in den jeweiligen Abschnitten nur Aktionen auswählen, die auf den Abschnitt übertragen werden können (so können Sie beispielsweise "Softwareverteilung" nicht als eine Aktion für den Abschnitt "Vor der Installation..." auswählen). Sie können jede verfügbare Aktion jedem Abschnitt hinzufügen. Beachten Sie jedoch, dass einige Aktionen, wenn sie in der falschen Reihenfolge ausgeführten werden, die Funktionsfähigkeit der Vorlage kompromittieren oder Ihr System unbrauchbar machen können.

Schritt 3: Erstellen eines Zeitplans für die Bereitstellung der Vorlage

Ein Versorgungstask umfasst Vorlagen und die Gerätekennungen der Zielgeräte. Zu Beginn des Versorgungstasks wird der Auftrag mit dem Computerdatensatz des Geräts in der Datenbank verknüpft, damit der Konfigurationsverlauf mit dem Computer verbunden bleibt. Konfigurationstasks können nicht für andere Zielgeräte wieder verwendet werden; sie können jedoch wieder verwendet werden, indem eine andere Gerätekennung angegeben wird.

Das Extra **Geplante Tasks** zeigt den Status eines geplanten Tasks an und wird während der Taskausführung und nach Abschluss des Tasks eingeblendet. Der Scheduler-Dienst kann auf zwei Arten mit Geräten kommunizieren: Über den Standard Management Agent (der bereits auf Geräten installiert sein muss) oder über ein Systemkonto auf Domänenebene. Auf dem von Ihnen ausgewählten Konto muss das Protokoll als Dienstprivileg installiert sein und Sie müssen Anmeldeinformationen unter "Dienste konfigurieren" angegeben haben.

Erstellen einer Versorgungsvorlage

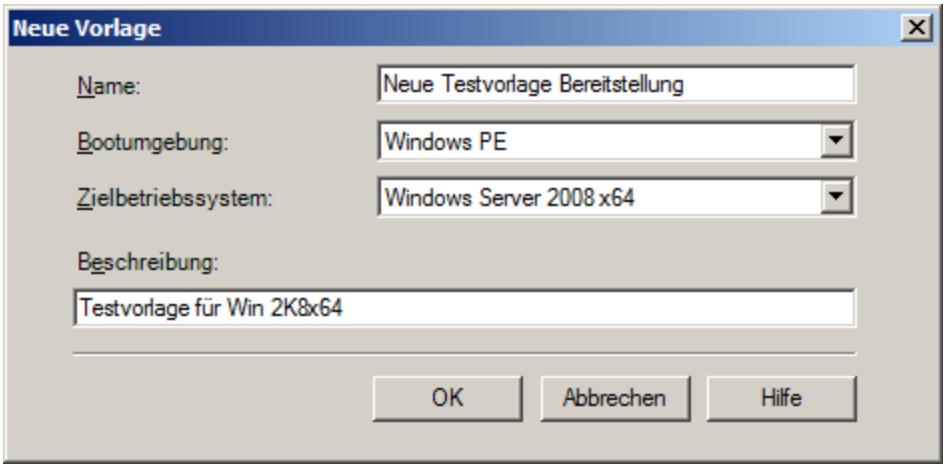
Das Dialogfeld **Neue Versorgungsvorlage** verwenden Sie, um eine Versorgungsvorlage zu erstellen.

Eine Vorlage ist eine Abfolge von Aktionen oder Bausteinen, die auf einen Server in einer festgelegten Reihenfolge anzuwenden sind. Eine Vorlage kann eine oder eine Vielzahl von Aktionen umfassen. Die Taskreihenfolge in einer Vorlage kann geändert werden. Die Aktionssequenz kann nur dort geändert werden, wo es Sinn macht (Sie können beispielsweise keine Aktion, die im Anschluss an die Installation des Betriebssystems auszuführen ist, vor die Installation des Betriebssystems platzieren).

Es gibt mehrere vorkonfigurierte Vorlagen für unterschiedliche Anbieter (HP, Dell usw.). Vorlagen werden als XML-Dateien in der Datenbank gespeichert.

So erstellen Sie eine Vorlage

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Gruppe **Versorgungsvorlagen** auf den Ordner **Öffentlich** oder auf den Ordner **Eigene Vorlagen**.
3. Klicken Sie in der Symbolleiste auf **Neue Versorgungsvorlage**.



4. Geben Sie einen beschreibenden Namen in das Feld **Name** ein.

5. Geben Sie eine Beschreibung in das Feld **Beschreibung** ein. Name und Beschreibung werden in Spalten in der Liste der Vorlagen angezeigt.
6. Wählen Sie die Windows PE-Prebootumgebung.
7. Wählen Sie ein Zielbetriebssystem für die Vorlage aus.
8. Klicken Sie auf **OK**.

Um Vorlageneigenschaften zu ändern, doppelklicken Sie auf die Vorlage oder klicken Sie mit der rechten Maustaste auf die Vorlage und wählen Sie **Eigenschaften** aus.

Löschen einer Versorgungsvorlage

Sie können nur Vorlagen löschen, die zuvor noch nicht ausgeführt (gesperrt) wurden und die nicht Bestandteil anderer Vorlagen sind. Gesperrte Vorlagen können aus der Liste gelöscht (entfernt) werden, bleiben aber in der Datenbank.

So löschen Sie eine Versorgungsvorlage

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Gruppe **Versorgungsvorlagen** auf den Ordner **Öffentlich** oder auf den Ordner **Eigene Vorlagen**.
3. Wählen Sie eine Vorlage aus und klicken Sie auf **Löschen**.
4. Klicken Sie auf **Ja**.

Konfigurieren einer Versorgungsvorlage

1. Doppelklicken Sie auf eine Versorgungsvorlage.
2. Klicken Sie im linken Navigationsfenster auf **Aktionsliste**.
3. Wählen Sie im mittleren Fensterausschnitt den Abschnitt aus, in dem die Aktion stattfinden soll.
    - **Systemmigration:** Funktionen und Komponenten, die vor Systemänderungen gespeichert werden müssen (oder vor dem Migrieren eines Geräts auf eine andere Hardware oder ein virtuelles Gerät). Dieser Abschnitt kann beispielsweise eine Aktion zur Erfassung von Profilinformationen bei der Migration zu Windows Vista enthalten.
    - **Vor der Installation des Betriebssystems:** Aktionen, die durchgeführt werden, wenn das Gerät in eine Vorinstallationsumgebung (Windows PE) gebootet wird. Bei einem Server würden Sie beispielsweise in diesem Abschnitt die RAID-Konfiguration hinzufügen.
    - **Betriebssystem-Installation:** Aktionen, die in der Vorinstallationsumgebung (Windows PE) bei der Installation des Betriebssystems ausgeführt werden.
    - **Nach der Installation des Betriebssystems:** Aktionen, die nach der Betriebssysteminstallation im Zielbetriebssystem durchgeführt werden, wie beispielsweise die Durchführung eines Patchmanagement-Tasks.
    - **Systemkonfiguration:** Installation/Ausführung zusätzlicher Anwendungen und Systemkonfiguration im installierten Betriebssystem. Beispielsweise die Treiberinstallationstasks in diesem Abschnitt.
4. Klicken Sie auf **Hinzufügen**.
5. Geben Sie einen spezifischen Namen für die Aktion in das Feld **Name** ein.
6. Geben Sie eine detaillierte Beschreibung der Aktion in das Feld **Beschreibung** ein.

7. Wählen Sie in der Liste **Typ** einen Aktionstyp aus.
8. Klicken Sie unter **Aktionsvariablen** auf **Hinzufügen**, um eine Variable hinzuzufügen, die nur für diese Aktion gilt. Geben Sie die Werte in die Textfelder ein, wählen Sie den Variablentyp aus und klicken Sie auf **OK**.
9. Füllen Sie unter **Ausgewählte Aktionseigenschaften** die für den Aktionstyp erforderlichen Datenfelder aus. Diese Daten variieren je nachdem, welchen Aktionstyp Sie ausgewählt haben.
10. Wenn Sie die Aktion definiert haben, klicken Sie auf **Übernehmen**, um sie zu speichern und mit der Bearbeitung der Vorlage fortzufahren. Wenn Sie mit der Vorlagendefinition fertig sind, klicken Sie auf **OK**.

Planen eines Versorgungstasks

So planen Sie einen Versorgungstask

1. Wählen Sie im Extra **Betriebssystembereitstellung** ein Vorlage aus einem der Order **Versorgungsvorlagen** aus.
2. Klicken Sie auf die Schaltfläche **Vorlage planen** in der Symbolleiste.

   Das Extra "Geplante Tasks" wird mit einem Task für die Versorgungsvorlage geöffnet.
3. Wählen Sie in der Netzwerkansicht die Geräte aus, für die Sie den Versorgungstask bereitstellen werden. Ziehen Sie die Geräte auf das Extra **Geplante Tasks** und legen Sie sie auf dem Versorgungstask ab.
4. Klicken Sie mit der rechten Maustaste auf den Versorgungstask und wählen Sie **Eigenschaften** aus. Wählen Sie eine Zeitplanoption aus und klicken Sie auf **Speichern**.

Wenn Sie auf **Vorlage planen** klicken, wird ein Task erstellt (er verfügt über keine Zielgeräte und keinen Zeitplan). Wenn Sie keine Zielgeräte hinzufügen oder einen Zeitplan für den Task definieren, beachten Sie, dass der Task in der Taskliste verbleibt, bis Sie ihn eingeplant oder gelöscht haben.

Im Extra **Geplante Tasks** werden Tasks in folgenden Ordnern gruppiert:

- **Eigene Tasks:** Tasks, für die Sie einen Zeitplan erstellt haben. Nur Sie selbst und administrative Benutzer von Management Suite können diese Tasks sehen.
- **Öffentliche Tasks:** Tasks, die von Benutzern als "öffentlich" gekennzeichnet wurden. Jeder Benutzer, der für einen Task aus dieser Kategorie einen Zeitplan erstellt, wird Eigentümer dieses Tasks. Der Task verbleibt im Ordner **Öffentliche Tasks** und ist auch in der Gruppe **Benutzertasks** für diesen Benutzer sichtbar.
- **Alle Tasks:** Sowohl eigene als auch öffentliche Tasks.
- **Benutzertasks** (nur administrative Benutzer von Management Suite): Alle Tasks, die von Benutzern erstellt wurden.

Meldungen an den Benutzer bei der Taskausführung

Wenn ein Versorgungstask auf einem Gerät ausgeführt wird und eine der Versorgungsaktionen einen Neustart umfasst, wird die Ausführung des Tasks fortgesetzt, nachdem das Gerät neu gestartet wurde. Der Benutzer wird nach dem Neustart zur Anmeldung aufgefordert, und wenn die Anmeldung abgeschlossen ist, gibt eine Statusmeldung Aufschluss über den Fortschritt des Tasks.

Wenn der Benutzer beim Starten des Versorgungstask nicht angemeldet ist, wird der Task ohne Eingaben des Benutzers ausgeführt. Gehört eine Neustartaktion zum Umfang des Tasks, wird dieser auch ohne Anmeldung des Benutzers weiter ausgeführt.

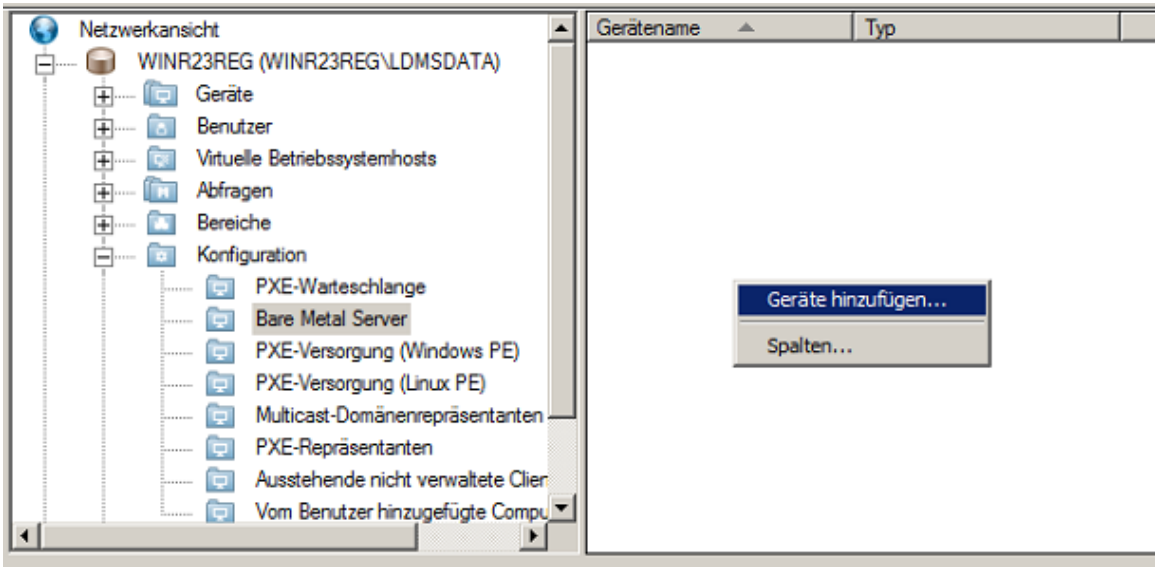
Meldet sich der Benutzer an, während der Versorgungstask ausgeführt wird, erhält er eine Statusmeldung, die ihn davon in Kenntnis setzt, dass ein Task ausgeführt wird und wie es um den Fortschritt des Tasks steht. Bitte beachten Sie, dass Statusmeldungen nur zwischen Aktionen aktualisiert werden. Wenn mit einem Task eine zeitaufwändige Aktion abgearbeitet wird, beispielsweise die Installation einer umfangreichen Anwendung, dann kann der Eindruck entstehen, dass die Fortschrittsanzeige stehengeblieben ist. Ist die Aktion dann abgeschlossen, wird jedoch der Status aktualisiert.

Versorgung von Bare-Metal-Geräten

Versorgung ermöglicht die Versorgung von Bare-Metal-Geräten. Sie können diesen Vorgang starten, bevor die Geräte tatsächlich zur Verfügung stehen. Hierzu geben Sie eine Hardwarekennung (wie beispielsweise die GUID oder MAC-Adresse) für jedes neue Gerät im Order **Konfiguration > Bare-Metal-Server** in der Netzwerkansicht ein. Sie können mehrere Geräte auf einmal hinzufügen, indem Sie mit einer .csv-Datei eine Liste mit Gerätekennungen importieren. Die für den automatisierten Versorgungsagenten (ldprovision) benötigten Informationen werden in der Datenbank aufgezeichnet.

So versorgen Sie Bare-Metal-Geräte

1. Klicken Sie in der Netzwerkansicht auf **Konfiguration > Bare-Metal-Server**.
2. Klicken Sie mit der rechten Maustaste auf die Geräteliste und wählen Sie **Geräte auswählen** aus.



3. Um Daten zu einzelnen Geräten hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie eine Namen für die Geräte ein, die Sie hinzufügen werden (dies kann entweder ein Name zur Beschreibung einer Gruppe von Geräten oder nur für ein einzelnes Gerät sein).
4. Wählen Sie einen Typ aus der Liste **Kennungstyp** aus.
5. Geben Sie die Kennung für jedes Gerät ein und klicken Sie auf **Hinzufügen**, um diese zur Liste hinzuzufügen.

6. Zum Importieren der Gerätedaten wählen Sie einen Typ aus der Liste **Kennungstyp** aus. Geben Sie das Laufwerk, den Pfad und Dateinamen der Importdatei ein oder verwenden Sie Durchsuchen, um den Namen zu finden und auszuwählen. Klicken Sie auf **Importieren**.
7. Verknüpfen Sie jedes Gerät einzeln mit einer Versorgungsvorlage.
8. Stecken Sie die Geräte ein und stellen Sie darauf eine IdProvision-Boot-CD oder ein bootfähiges USB-Laufwerk bereit oder konfigurieren Sie das BIOS auf Netzwerk/PXE-Boot.
9. Fahren Sie die Geräte hoch.

Erstellen von Bootmedien

Zur Erstellung von Bootmedien, die für die Versorgung von Geräten verwendet werden können, verwenden Sie das Dialogfeld "LANDesk Bootmedienerstellung". Die Versorgungskomponente erstellt ein physikalisches Medium, mit dem sich der Server in eine Prebootumgebung booten lässt. Dieses Speichermedium kann über einen PXE-Server oder ein bootfähiges USB-Gerät/CD/DVD bereitgestellt werden.

Eine Prebootumgebung besteht aus einem Betriebssystem, das über Video- und Netzwerkfunktionen, über einen reduzierten Inventarscanner sowie über einen Agenten verfügt, der Dateien empfangen und Befehle ausführen kann. Damit die Startmedien funktionieren, müssen Sie ein Zielgerät zum Starten vom richtigen Medium aus konfigurieren (im BIOS aktivieren Sie Netzwerk IPXE oder CD/DVD-Boot).

So erstellen Sie Imaging-Bootmedien

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Versorgungs-Bootmedien erstellen**.
3. Wählen Sie den **Bootmedientyp** aus (bootfähiges ISO-Laufwerk oder bootfähiges USB-Laufwerk). Wenn Sie "USB-Laufwerk" ausgewählt haben, setzen Sie das USB-Laufwerk ein und wählen Sie den Laufwerksbuchstaben. Wenn Sie "Bootfähige ISO" gewählt haben, wählen Sie einen Zielpfad aus, in dem die ISO gespeichert wird.
4. Klicken Sie auf **Erstellen**.

Die Erstellung von Bootmedien kann fehlschlagen, wenn die Speicherkapazität des Systems erschöpft ist.

HINWEIS: Die Erstellung von USB-Bootmedien erfordert Administratorrechte. Im Falle von Microsoft Vista müssen Sie das Programm downloaden und als Administrator ausführen.

HINWEIS: Um ein ISO-Medium zu erstellen, muss das Gerät, auf dem das Erstellungstool für Bootmedium ausgeführt wird, über IMAP2 verfügen, welches Sie von Microsoft über http://support.microsoft.com/kb/kb932716 erhalten.

Freigeben von Vorlagen

Die Symbolleistenschaltfläche **Vorlagen importieren** verwenden Sie, um Vorlagen im XML-Format zu importieren. Wenn Sie eine Vorlage importieren, wird eine Kopie der Vorlage im Ordner **Eigene Vorlagen** gespeichert. Anschließend können Sie den XML-Code der Vorlage bearbeiten, um deren Inhalt zu ändern.

Sie können eine Vorlage auch exportieren, um Sie als neue Datei zu speichern und diese Vorlagendatei dann für andere Benutzer freigeben.

So importieren Sie eine Vorlage

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Vorlagen importieren**.
3. Um eine Vorlage zu exportieren, geben Sie den Pfad und Dateinamen der XML-Datei in das Textfeld **Importdatei** ein; oder Sie klicken auf **Durchsuchen** und wählen die Datei aus.
4. Klicken Sie auf **Importieren**. Damit wird die Vorlage in den Ordner **Eigene Vorlagen** importiert.

Die Datei wird als .xtp-Datei gespeichert (XML-Vorlagenseite). Im Ordner **Eigene Vorlagen** wird die importierte Vorlage mit dem ursprünglichen Dateinamen gefolgt vom Datum und Uhrzeit des Imports aufgelistet.

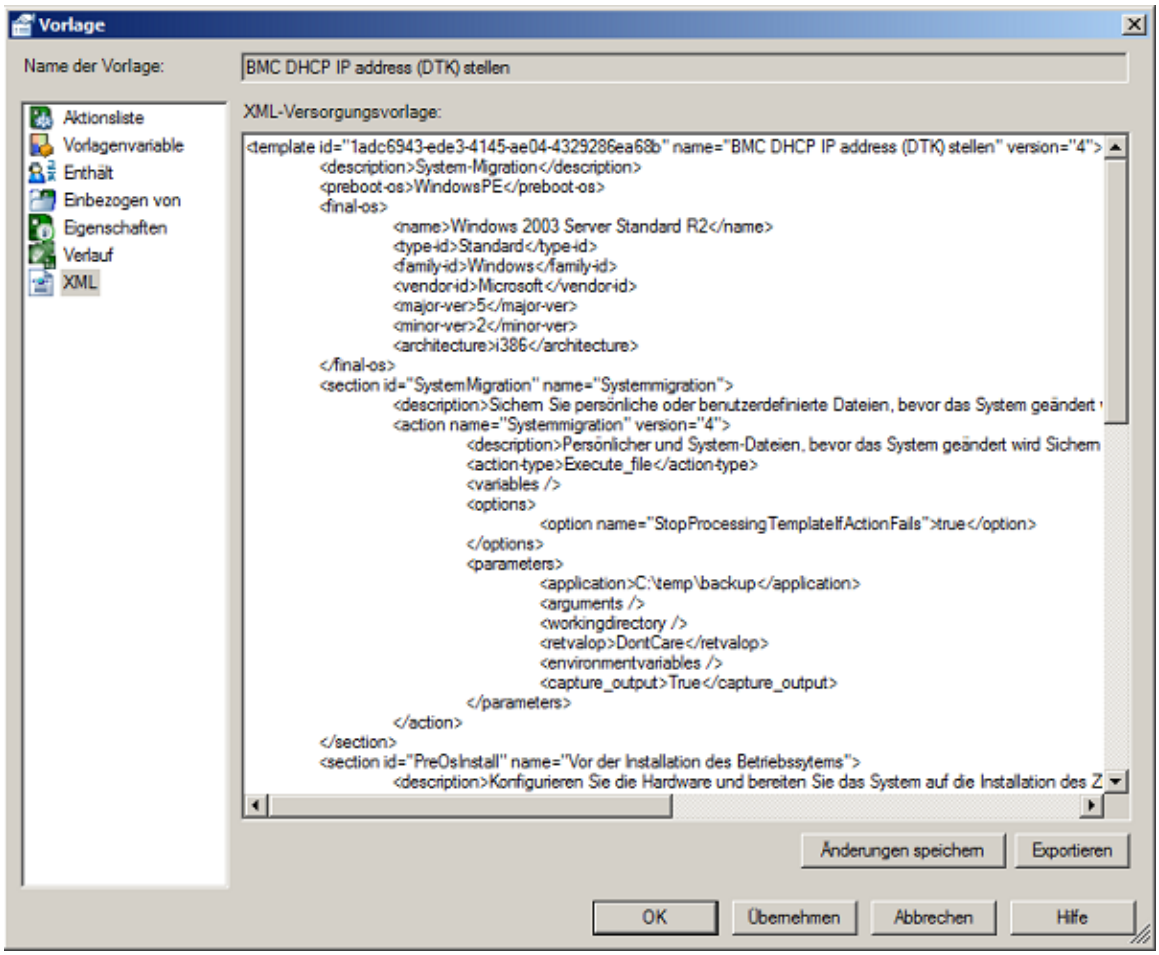
So exportieren Sie eine Vorlage

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie **Öffentlich** oder **Eigene Vorlagen** oder eine Untergruppe aus.
3. Doppelklicken Sie auf eine Vorlage. Klicken Sie in der Vorlagenansicht auf **XML**.
4. Klicken Sie auf **Exportieren**. Wählen Sie das Verzeichnis aus, in dem Sie die Vorlage speichern möchten, und klicken Sie auf **Speichern**.

Die Datei wird als .xtp-Datei gespeichert (XML-Vorlagenseite). Wenn Sie eine Vorlage exportieren, die nur UTF-Zeichen enthält, wird der Titel in Internet Explorer nicht korrekt angezeigt. Die nicht darstellbaren Zeichen im Vorlagentitel erscheinen als Unterstriche. Sie können den Vorlagentitel über das Dialogfeld **Speichern unter** ändern.

Ändern des XML-Codes einer Vorlage

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie **Öffentlich** oder **Eigene Vorlagen** oder eine Untergruppe aus.
3. Doppelklicken Sie auf eine Vorlage. Klicken Sie in der Vorlagenansicht auf **XML**.
4. Nehmen Sie die gewünschten Änderungen am XML-Code für die Vorlage vor.
5. Klicken Sie auf **Änderungen speichern**.
6. Um eine Kopie der Vorlage zu exportieren, klicken Sie auf **Exportieren** und geben einen Speicherort für die Datei an.
7. Klicken Sie auf **OK**, um die Vorlagenansicht zu schließen.



Versorgungsvorlagen sind entsprechend dem folgenden allgemeinen XML-Format strukturiert.

```
<template name= >

    <description></description>

    <section name= >

        <description></description>
        <action></action>

    </section>

    <section name= >

        <description></description>
        <action></action>

    </section>

</template>
```

Verwenden von vordefinierten Vorlagen

Die Schaltfläche **Vorlagen aktualisieren** verwenden Sie für den Download von vordefinierten Vorlagen, die für spezielle Systemhardware und allgemeine Versorgungstasks optimiert sind. Nachdem die Dateien heruntergeladen sind, importieren Sie diese und speichern sie dann im Order "Eigene Vorlagen".

Unter Umständen stehen zu einem späteren Zeitpunkt neue Vorlagen zur Verfügung, daher können Sie Vorlagen auch mehrmals herunterladen, wenn Sie eine Vorlage aktualisieren oder neue Vorlagen hinzufügen wollen.

Vorlagen werden auf LANDesk Servern zum Download bereitgestellt. Wählen Sie den Server aus, der ihrem Standort am nächsten ist. Im Dialogfeld **Vorlagen aktualisieren** können Sie außerdem Proxyservereinstellungen definieren, wenn Sie für den externen Zugriff einen Proxyserver verwenden.

HINWEIS: Während ein geplanter Aktualisierungstask für Vorlagen läuft, werden die aktuellen Einstellungen aus dem Dialogfeld "Vorlagen aktualisieren" verwendet, nicht die Einstellungen, die zum Zeitpunkt der Taskerstellung galten.

Klicken Sie hier, um Beschreibungen der Optionen für **Vorlagen aktualisieren** anzuzeigen.

Registerkarte "Neueste Vorlagen downloaden"

- **Website der Downloadquelle auswählen:** Gibt an, auf welchen Inhaltsserver für Versorgungsvorlagen zugegriffen wird, um die Datenbank mit den neuesten Versorgungsvorlagen zu aktualisieren. Wählen Sie den Server aus, der Ihrem Standort am nächsten ist.
- **Zu aktualisierende Versorgungsvorlagen auswählen**: Weist aus, auf welchen Plattformen Versorgungsvorlagen aktualisiert werden. Sie können eine oder mehrere Plattformen auswählen. Je mehr Plattformen Sie auswählen, umso länger dauert der Download.
- **Als neue Kopie importieren (neue Vorlage erstellen):** Importiert die Vorlagen als neue Vorlagen, ohne vorhandene Vorlagen oder Gruppen zu überschreiben.

Registerkarte "Proxyservereinstellungen"

Wenn Ihr Netzwerk einen Proxyserver für externe Übertragungen (z. B. Internetzugriff) nutzt, aktivieren und konfigurieren Sie auf dieser Registerkarte die Einstellungen für den Proxyserver. Internetzugang ist erforderlich, damit Informationen über Versorgungsvorlagen aktualisiert werden können.

- **Proxyserver verwenden:** Aktiviert die Proxyserver-Option (die Option ist standardmäßig deaktiviert). Wenn Sie einen Proxyserver aktivieren, müssen Sie die Adresse und den Port in die unten stehenden Felder eingeben.
  - **Adresse:** Gibt die IP-Adresse Ihres Proxyservers an.
  - **Port:** Gibt die Portnummer Ihres Proxyservers an.
- **HTTP-basierter Proxy:** Aktiviert den Proxyserver, wenn es sich um einen HTTP-basierten Proxy handelt (wie z. B. Squid), damit der Server Verbindungen mit FTP-Sites herstellen und von diesen Sites Patches downloaden kann. (Auf bestimmten FTP-Sites bereitgestellte Patches können erst dann über einen HTTP-basierten Proxy gedownloadet werden, wenn Sie zuvor diese Option aktivieren.)
- **Erfordert Anmeldung:** Ermöglicht die Eingabe eines Benutzernamens und eines Kennworts, wenn der Proxyserver Anmeldeinformationen verlangt und kein transparenter Proxyserver ist.

- **Benutzername:** Geben Sie einen gültigen Benutzernamen und Anmeldeinformationen für die Authentifizierung gegenüber dem Proxyserver ein.
- **Kennwort:** Geben Sie das Kennwort des Benutzers ein.

Download und Import von vordefinierten Vorlagen

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Vorlagen aktualisieren**.
3. Falls erforderlich, klicken Sie auf die Registerkarte **Proxyservereinstellungen** und geben Sie Proxyservereinstellungen an.
4. Wählen Sie eine Website der Downloadquelle aus.
5. Wählen Sie die herstellerspezifischen Vorlagen aus, die Sie downloaden möchten.
6. Markieren Sie das Kontrollkästchen **Als neue Kopie importieren (neue Vorlage erstellen)**, um die heruntergeladenen Vorlagen separat zu speichern, ohne dabei vorhandene Vorlagen oder Gruppen mit demselben Namen zu überschreiben.
7. Klicken Sie auf **Downloaden**. Wenn die Vorlagen heruntergeladen werden, wird eine Erfolgsmeldung angezeigt.
8. Klicken Sie auf **Importieren**, um die Vorlagen in den Ordner **Eigene Vorlagen** zu verschieben.

Verwenden von Installationsskripten in Versorgungsvorlagen

Die Registerkarte **Installationsskripte** verwenden Sie, um auf der Grundlage eines oder mehrerer Skripte eine Vorlage zu erstellen. Installationsskripte stellen Installationsskripte zur Verwendung beim Erstellen skriptgesteuerter Installationsaktionen in Vorlagen zur Verfügung. Es werden Batchdatei-Skripte, Shell-Skripte und viele andere Skripte unterstützt.

Die Aktionen "Abbild bereitstellen", "Skriptgesteuerte Installation" und "Skript injizieren" verwenden Skripte wie sysprep.inf oder unattend.txt. Mit "Skripte installieren" können Sie auch Variablen in Ihre Skripte einfügen. So kann beispielsweise ein Gerätename in eine sysprep.inf-Datei eingefügt werden.

Verwendung von Variablen

Installationsskripte unterstützen mehrere Schlüsselwertpaare, z. B.:

Variable	Beschreibung
%ldHostname%	Der Hostname
%ldDeviceID%	GUID des Geräts

Wenn es in der win.inf-Datei ein Schlüsselwertpaar gibt, das bereits als eine benutzerdefinierte Variable vorhanden ist, wird es von den Installationsskripten durch die benutzerdefinierte Variable ersetzt.

Um Variablen per Installationsskript als Variable zu übergeben (nicht durch den Versorgungsprozess zu ersetzen), setzen Sie die Variable in doppelte Prozentzeichen (zum Beispiel: `%%variable%%`).

Hinweise zur Verwendung von Skripten

- In Windows muss eine gültige, aktive, formatierte Partition vorhanden sein, damit die skriptgesteuerte Aktion stattfinden kann.

- Die Netzwerkinstallationsquelle muss ordnungsgemäß mit Treibern für das Zielgerät injiziert werden oder muss in den PnP-Treiberpfad des OEM eingefügt werden (zusätzliche Informationen können Sie im Installationshandbuch von Microsoft nachschlagen).
- Derzeit wird nur eine Befehlszeileninstallation unter Verwendung von winnt32 unterstützt.
- Die Datei "cmdlines.txt" wird dazu verwendet, Befehle an den letzten Betriebssystemstart anzuhängen.
- PXE/RIS wird nicht unterstützt.
- Schlägt die Installation fehl, können Sie zwecks Behebung des Fehlers im Ordner \ManagementSuite\ldlogon\provisioning\config nachsehen, wie das Installationsskript mit den ausgetauschten Variablen aussieht. Diese Strategie kann auch immer dann angewendet werden, wenn ein Skript geändert wird oder ein Skript in den Aktionen "Skript injizieren" oder "Abbild bereitstellen" zum Einsatz kommt.
- Das temporäre Verzeichnis für die Versorgung ist %systemdrive%/ldprovisioning.

Linux-Installationsprobleme

Skriptgesteuerte Linux-Installationen werden nur unter Verwendung des PXE-Bootvorgangs unterstützt.

Beachten Sie beim Ausführen einer skriptgesteuerten Installationsaktion für Linux, dass jede Linux-Version darüber wacht, ob Sie die korrekte CD verwenden, wenn Sie mit der Installation beginnen. Aus diesem Grund benötigen Sie eine unterschiedliche initrd und linux (vmlinuz) für jede Version von Linux.

Die beste Möglichkeit, dieser Anforderung nachzukommen, besteht darin, die Boot-Abbilder von der jeweiligen CD in die PXE zu kopieren und sie umzubenennen. Sie sollten sie nach \LANDesk\PXE\System\images\x86pc\undi\provlinux kopieren. Benennen Sie im Falle von Red Hat 4 die Dateien beispielsweise in initrd.rh4as und vmlinuz.rh4 um, und für Sles10 in initrd.sles10 und linux.sles10. Verwenden Sie dann beim Erstellen einer skriptgesteuerten Installationsaktion die korrekte initrd.xxx und xxxlinux.xxx in der skriptgesteuerten Installationsvorlage.

Linux-Installationsskripte unterstützen zahlreiche Schlüsselwertpaare, z. B.:

Variable	Beschreibung
ldDNSDomain	Die DNS-Domäne
ldInstallServer	Der Quellserver der Installation
ldInstallDir	Das Installationsverzeichnis. Beispiel: /storage/OS/linux/redhat/enterprise_4as/u3/i386/
ldNameserver1	DNS-Server 1
ldNameserver2	DNS-Server 2

Importieren und Exportieren von Installationsskripten

So importieren Sie ein Installationsskript

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Installationsskripte**.

3. Geben Sie den Pfad- und Dateinamen des Skripts in das Textfeld **Dateiname** ein oder klicken Sie auf **Durchsuchen**, navigieren Sie zum Skript, wählen Sie es aus und klicken Sie auf **Öffnen**.
4. Geben Sie einen Namen für das Skript in das Feld **Skriptname** ein. Dieser Name wird in diesen Dialogfeld in der Liste **Installationsskripte** angezeigt.

   Der Name wird ferner in der Liste **Installationsskripte** angezeigt, wenn Sie eine skriptgesteuerte Installationsaktion zur einer Versorgungsvorlage hinzufügen.
5. Geben Sie zusätzliche Details zum Skript in das Feld **Beschreibung** ein.
6. Wählen Sie das Zielbetriebssystem in der Liste **Zielbetriebssystem** aus.
7. Aktivieren Sie das Kontrollkästchen **Variablen in Skript einfügen**, wenn Sie beim Importieren des Skripts Variablen austauschen möchten. Beim Ersetzen von Variablen werden öffentliche Variablen automatisch ersetzt. Zusätzliche benutzerdefinierte Variablen werden unterstützt und die Werte werden ersetzt, sobald die Vorlage ausgeführt wird.
8. Klicken Sie auf **Importieren**, um das Skript in die Liste **Installationsskripte** zu stellen.

So exportieren Sie ein Installationsskript

1. Wählen Sie das Skript im Dialogfeld **Installationsskripte** in der Liste **Installationsskripte** aus.
2. Klicken Sie auf **Exportieren**. Geben Sie einen Dateinamen und einen Speicherort ein und klicken Sie auf **Speichern**.

Versorgungsverlauf

Mit der Option "Versorgungsverlauf" können Sie den Verlauf einer Versorgungsvorlage anzeigen. Dies gibt Ihnen die Möglichkeit, den Status eines bestimmten Tasks zu überprüfen, festzustellen, wie ein bestimmter Server versorgt wurde, oder herauszufinden, welche Server mit einer bestimmten Vorlage versorgt wurden. Während der Versorgung eines Systems werden alle Aktionen im Versorgungsverlauf aufgezeichnet.

Wenn Sie ein System in einen bekannten Zustand zurückversetzen möchten, können Sie die Vorlage, mit der dieser bekannte Zustand wiederhergestellt wird, erneut ausführen. Wenn Sie eine Vorlage erneut ausführen möchten, sollten Sie berücksichtigen, dass bestimmte Aktionen externer Bestandteil der Versorgungskomponente sind. Speichern Sie alle Softwareverteilungspakete, Agentenkonfigurationen und Programme, die Sie in Verbindung mit einer Vorlage downloaden und ausführen. Andernfalls können diese Elemente nicht erneut ausgeführt werden.

So zeigen Sie den Versorgungsverlauf einer Vorlage an

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf den Ordner **Öffentlich** oder auf den Ordner **Eigene Vorlagen**, um Vorlagen anzuzeigen.
3. Doppelklicken Sie auf eine Vorlage.
4. Klicken Sie auf **Verlauf**.
5. Klicken Sie in der Spalte **Taskname** auf einen Namen und klicken Sie dann auf **Auswählen**, um Details zu diesem Task anzuzeigen.

HINWEIS: Wenn die Vorlage niemals ausgeführt wurde, gibt es keine Verlaufsdaten.

So zeigen Sie den Versorgungsverlauf nach Task sortiert an

1. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
2. Klicken Sie unter **Eigene Tasks** oder **Öffentliche Tasks** auf den Tasknamen.
3. Klicken Sie auf eine der Kategorien unter dem Task (Alle Geräte, Aktiv, Ausstehend, Erfolgreich oder Fehlgeschlagen). In diesen Kategorien sind Zielcomputer entsprechend dem Status der Versorgungstask auf dem jeweiligen Gerät aufgeführt.
4. Klicken Sie auf einen Zielcomputer und wählen Sie **Versorgungsverlauf** aus.
5. Klicken Sie auf **Eigenschaften**, um die Eigenschaften der Versorgungsvorlage anzuzeigen.
6. Erweitern Sie einen Vorlagenabschnitt und klicken Sie auf eine Aktion, um Einzelheiten zur Bereitstellung der Aktion anzuzeigen.

So zeigen Sie den Versorgungsverlauf nach Gerät an

1. Klicken Sie in der Netzwerkansicht auf **Eigene Geräte** oder auf **Öffentliche Geräte** und suchen Sie das Gerät.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und wählen Sie **Versorgungsverlauf** aus.
3. Klicken Sie auf einen Tasknamen und dann auf **Auswählen**, um Details zum Versorgungstask anzuzeigen.
4. Klicken Sie auf **Eigenschaften**, um die Eigenschaften der Versorgungsvorlage anzuzeigen.
5. Erweitern Sie einen Vorlagenabschnitt und klicken Sie auf eine Aktion, um Einzelheiten zur Bereitstellung der Aktion anzuzeigen.

HINWEIS: Um den aktuellen Status einer Vorlage zu erhalten, die derzeit ausgeführt wird, klicken Sie auf **Aktualisieren**, um den Verlaufsstatus zu aktualisieren.

Versorgungsvorlagengruppen

Mit Versorgungsvorlagengruppen können Sie Ihre Vorlagen auf unterschiedliche Weisen organisieren Sie können beispielsweise Gruppen auf der Basis spezifischer Anbieter und Untergruppen auf der Basis von Servermodellen erstellen. Wenn Sie dann zu einem späteren Zeitpunkt eine der Vorlagen in der Gruppe ändern möchten, müssen Sie die Vorlage lediglich aus der Gruppe entfernen und die bearbeitete Vorlage wieder der Gruppe hinzufügen. Untergruppen lassen sich bis zu sechs Ebenen tief schachteln.

So erstellen Sie eine Vorlagengruppe

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Wählen Sie **Öffentlich** oder **Eigene Vorlagen** aus.
3. Klicken Sie auf die Schaltfläche **Vorlagengruppe erstellen** in der Symbolleiste.
4. Geben Sie einen Namen für die Gruppe in das Feld **Gruppenname** ein.
5. Geben Sie eine Beschreibung in das Feld **Gruppenbeschreibung** ein.
6. Klicken Sie auf **OK**.

So löschen Sie eine Gruppe

1. Wählen Sie eine Gruppe aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Löschen**.
2. Klicken Sie auf **Ja** und bestätigen Sie dann, dass Sie die Gruppe löschen möchten.

HINWEIS: Eine Gruppe kann auch dann gelöscht werden, wenn sie nicht leer ist. Vergewissern Sie sich daher, dass eventuell in der Gruppe enthaltene Untergruppen und Vorlagen gelöscht werden können, bevor Sie die Löschung bestätigen.

Definieren des Abbildspeicherorts und des Abbilderstellungstools

Das Dialogfeld **Abbildspeicherort und Abbilderstellungstool auswählen** verwenden Sie, um auf den Speicherort des Abbilderstellungstools zu zeigen und um anzugeben, wo das Abbild gespeichert werden soll. Dieses Dialogfeld steht im Rahmen der Aktionen **Abbild erfassen** und **Abbild bereitstellen** zur Verfügung.

So definieren Sie den Abbildspeicherort und das Abbilderstellungstool

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf **Öffentlich** oder auf **Eigene Vorlagen**.
3. Doppelklicken Sie auf eine Vorlage.
4. Klicken Sie auf **Aktionsliste**.
5. Klicken Sie auf den Abschnitt **Betriebssystem-Installationen**.
6. Klicken Sie auf die Schaltfläche **Hinzufügen**.
8. Wählen Sie in der Liste **Aktionstyp** entweder **Abbild erfassen** oder **Abbild bereitstellen** aus. Geben Sie einen Namen für die Aktion ein und klicken Sie auf **OK**.
9. Klicken Sie auf **Assistenten starten**.
10. Wählen Sie in der Liste **Abbildtyp auswählen** den Abbildtyp aus, den Sie erfassen oder bereitstellen möchten.
11. Geben Sie den für die Abbilddatei zu verwendenden Speicherort an.
12. Geben Sie den Speicherort der Abbilderstellungsanwendung an.
13. Klicken Sie auf **OK**.

HINWEIS: Abbilder werden oft nicht auf dem Coreserver, sondern anderenorts gespeichert. Trifft dies zu, sollten Sie den Aktionen **Abbild erfassen** oder **Abbild bereitstellen** die Aktion **Laufwerk zuordnen** voranstellen, in der Sie die Authentifizierungsinformationen des Speicherorts angeben.

Versorgung mit Vorlagenvariablen

Vorlagenvariablen verbessern die Portierbarkeit und Anpassbarkeit von Vorlagen. Eine Vorlage kann beispielsweise sehr spezifische zu kopierende Dateinamen, Installationspfade oder eine IP-Adresse enthalten, aus der Dateien exportiert werden können. Mit Benutzervariablen anstelle dieser spezifischen Objekte kann die Vorlage jedoch mehr Situationen oder Gebietsschemata abdecken, indem die spezifischen Objekte ganz einfach durch Variablen im XML-Code ersetzt werden.

Es gibt vier Typen von Variablen. Diese sind (der Wichtigkeit nach geordnet):

- **Gerät:** Variablen, die einem bestimmten Gerät zugewiesen sind
- **Global:** Variablen, die für alle Vorlagen öffentlich (verfügbar) sind
- **Vorlage:** Variablen, die nur auf die zugeordnete Vorlage anwendbar sind
- **Aktion:** Variablen, die einer bestimmten Aktion zugewiesen sind

Bei Variablen muss auf Groß- und Kleinschreibung geachtet werden.

Verwandte Themen

"Definieren einer Gerätevariablen " auf Seite 462

"Definieren einer öffentlichen (globalen) Variablen" auf Seite 463

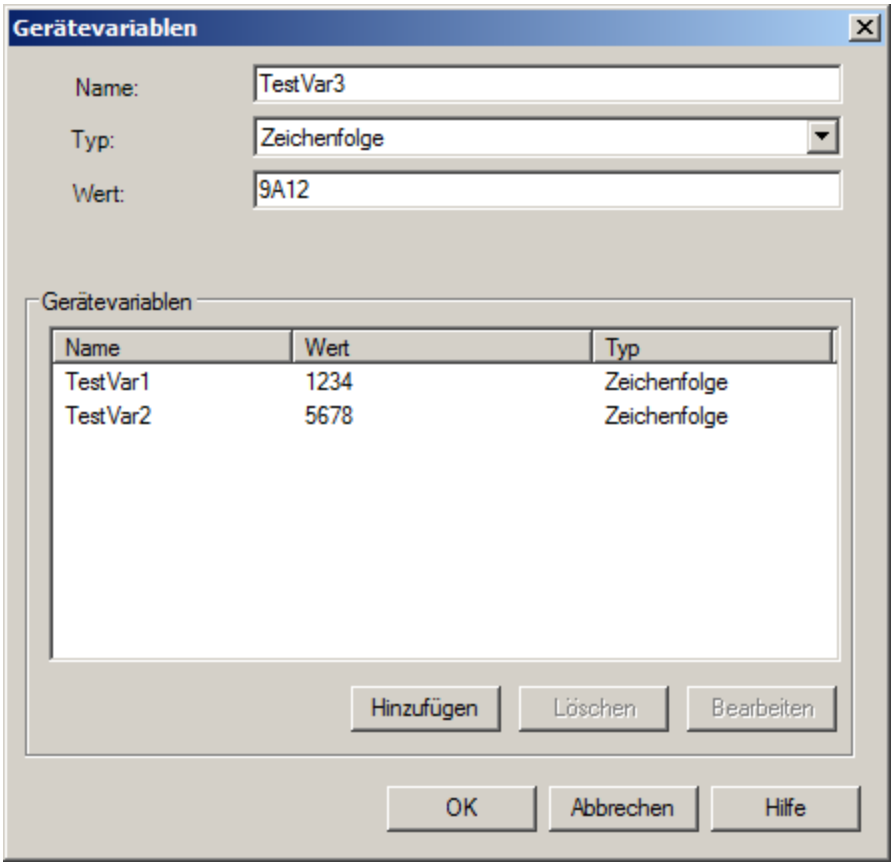
"Definieren einer Vorlagenvariablen" auf Seite 464

"Definieren einer Aktionsvariablen" auf Seite 465

"So erstellen Sie eindeutige Kennungen für neue Geräte " auf Seite 467

Definieren einer Gerätevariablen

1. Klicken Sie in der Liste **Alle Geräte** mit der rechten Maustaste auf ein Gerät und wählen Sie **Gerätevariablen verwalten** aus.



2. Geben Sie den Namen des Elements (z. B. IP-Adresse) in das Feld **Name** ein.
3. Geben Sie den zu ersetzenden Wert in das Feld **Wert** ein.
4. Wählen Sie den Typ aus.
   - **Zeichenfolge:** Geben Sie einen Zeichenfolgenwert ein
   - **Datenbankwert:** Geben Sie eine Datenbank-Kennungszeichenfolge ein, wie zum Beispiel Computer.Netzwerk."NIC-Adresse".
   - **Private Daten:** Geben Sie einen Wert ein, der in der Datenbank verschlüsselt werden muss.

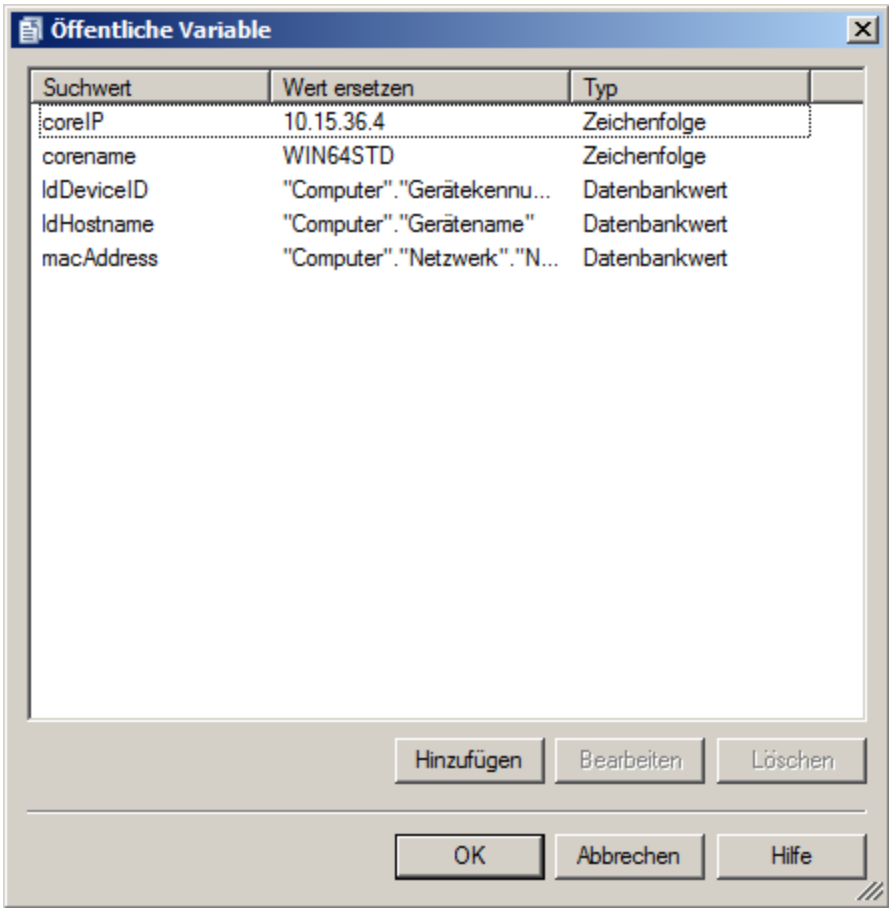
Verwenden Sie Anführungszeichen mit Leerstellen um den Namen. Sie können die meisten Werte aus der Inventardatenbank verwenden.

5. Klicken Sie auf **Speichern**.

Definieren einer öffentlichen (globalen) Variablen

Die Symbolleisten-Schaltfläche **Öffentliche Variablen** verwenden Sie zur Anzeige und Festlegung globaler Variablen, die für alle Versorgungsvorlagen gelten. Mithilfe solcher Variablen können Sie zu kopierende Vorlagendateinamen, Installationspfade oder IP-Adressen, aus denen Dateien exportiert werden sollen, anpassen. Benutzervariablen (Variablen, die nur für eine Vorlage gelten) haben gegenüber öffentlichen Variablen Vorrang.

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Öffentliche Variablen**.



3. Klicken Sie auf **Hinzufügen**, um eine Variable hinzuzufügen.
4. Geben Sie die Variable, die Sie hinzufügen möchten, in das Feld **Suchwert** ein (zum Beispiel: CoreIP).
5. Geben Sie den Wert, den Sie ersetzen möchten, in das Feld **Ersatzwert** ein. (Wenn beispielsweise der Suchwert "CoreIP" lautet, geben Sie die IP-Adresse ein, durch die CoreIP ersetzt werden soll.)
6. Wählen Sie den Typ aus.

- **Zeichenfolge:** Geben Sie einen Zeichenfolgenwert ein
- **Datenbankwert:** Geben Sie eine Datenbank-Kennungszeichenfolge ein, wie zum Beispiel Computer.Netzwerk."NIC-Adresse".
- **Private Daten:** Geben Sie einen Wert ein, der in der Datenbank verschlüsselt werden muss.

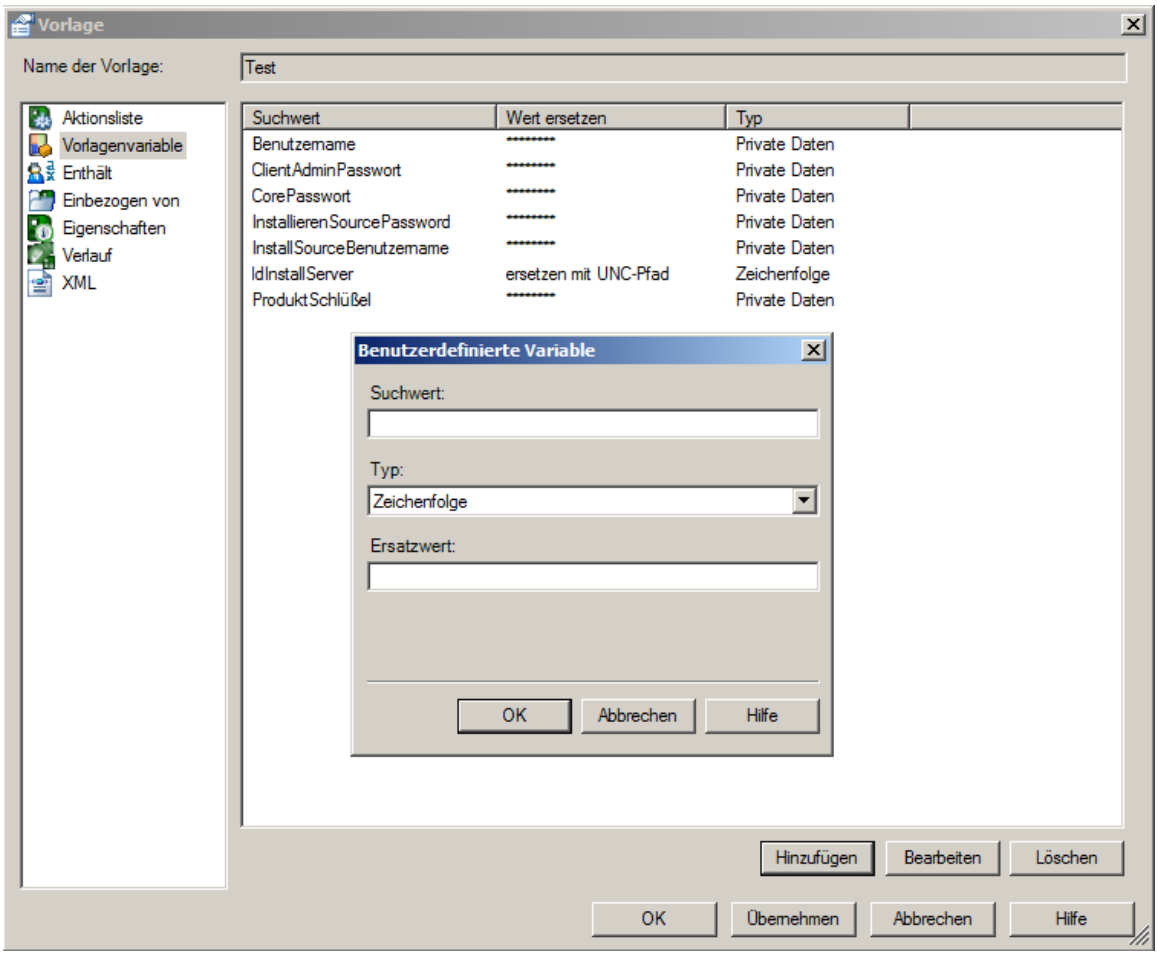
Verwenden Sie Anführungszeichen mit Leerstellen um den Namen. Sie können die meisten Werte aus der Inventardatenbank verwenden.

7. Klicken Sie auf **OK**.

Für die Abwicklung von Datenbanksuchen wird dem Ersatzwert ein "ldbnf:"-Präfix hinzugefügt. Die Datenbanktabelle und das Schlüsselpaar können dann zur Suche nach einem bestimmten Eintrag in der Datenbank verwendet werden. Die öffentliche ldDeviceID-Variable, die standardmäßig konfiguriert wird, ist ein Beispiel dafür, wie eine Datenbank-Suchvariable hinzugefügt wird.

Definieren einer Vorlagenvariablen

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf **Öffentlich** oder auf **Eigene Vorlagen**, um eine Liste von Vorlagen anzuzeigen.
3. Doppelklicken Sie auf eine Vorlage, um die Vorlagenansicht zu öffnen.
4. Klicken Sie auf **Vorlagenvariable**.



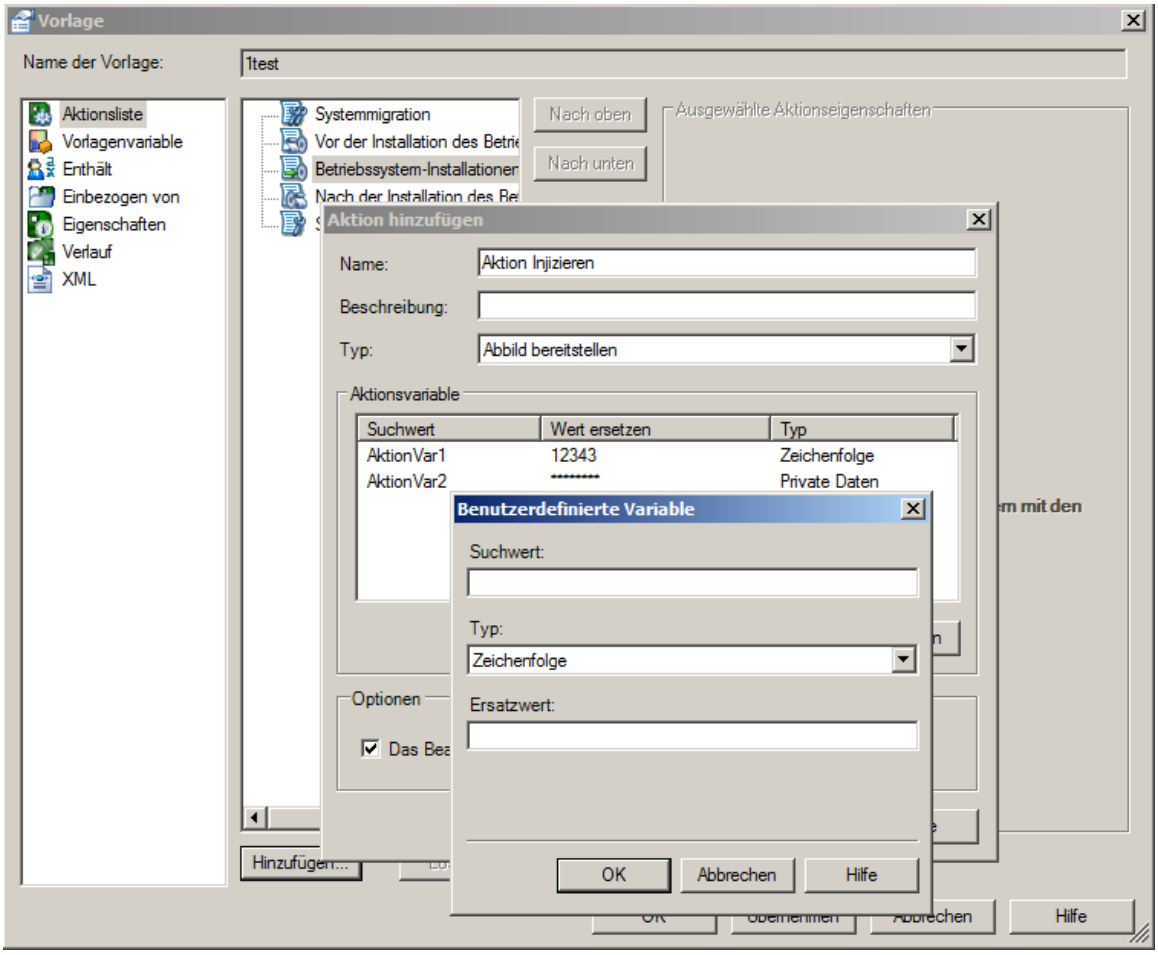
5. Klicken Sie auf **Hinzufügen**.
6. Geben Sie die Variable, die Sie hinzufügen möchten, in das Feld **Suchwert** ein.
7. Geben Sie den Wert, den Sie ersetzen möchten, in das Feld **Ersatzwert** ein.
8. Wählen Sie den Typ aus.
   - **Zeichenfolge:** Geben Sie einen Zeichenfolgenwert ein
   - **Datenbankwert:** Geben Sie eine Datenbank-Kennungszeichenfolge ein, wie zum Beispiel Computer.Netzwerk."NIC-Adresse".
   - **Private Daten:** Geben Sie einen Wert ein, der in der Datenbank verschlüsselt werden muss.

   Verwenden Sie Anführungszeichen mit Leerstellen um den Namen. Sie können die meisten Werte aus der Inventardatenbank verwenden.
9. Klicken Sie auf **OK**.

Definieren einer Aktionsvariablen

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie mit der rechten Maustaste auf eine Vorlage und dann auf **Bearbeiten**.

3. Klicken Sie auf **Aktionsliste** und wählen Sie einen Abschnitt, in dem Sie die Variable definieren werden.
4. Klicken Sie auf **Hinzufügen**, um eine neue Aktion zu erstellen. (Wenn Sie eine vorhandene Aktion ändern möchten, klicken Sie mit der rechten Maustaste auf die Aktion und wählen **Eigenschaften** aus.)
5. Klicken Sie auf **Hinzufügen**, um eine Aktionsvariable hinzuzufügen.



6. Geben Sie die Variable, die Sie hinzufügen möchten, in das Feld **Suchwert** ein.
7. Geben Sie den Wert, den Sie ersetzen möchten, in das Feld **Ersatzwert** ein.
8. Wählen Sie den Typ aus.
   - **Zeichenfolge:** Geben Sie einen Zeichenfolgenwert ein
   - **Datenbankwert:** Geben Sie eine Datenbank-Kennungszeichenfolge ein, wie zum Beispiel Computer.Netzwerk."NIC-Adresse".
   - **Private Daten:** Geben Sie einen Wert ein, der in der Datenbank verschlüsselt werden muss.

   Verwenden Sie Anführungszeichen mit Leerstellen um den Namen. Sie können die meisten Werte aus der Inventardatenbank verwenden.
9. Klicken Sie auf **OK**.

So erstellen Sie eindeutige Kennungen für neue Geräte

Um eindeutige Kennungen für neue Geräte zu erstellen verwenden Sie eine öffentliche Variable, die auf einer MAC-Adresse des Zielgerätes basiert, wie nachstehend gezeigt:

Variable (Datenbank) = macAdresse	Wert = Computer.Network. "NIC Adresse"
Variable (Zeichenfolge) = Präfix	Wert = UT (Benutzerwert wie Speicherort - Optional)
Variable (Zeichenfolge) = Suffix	Wert = XP (Benutzerwert wie Betriebssystem - Optional)
Variable (Zeichenfolge) = ComputerName	Wert = %Prefix%%MACaddr%%Suffix%

Im nächsten Schritt verwenden Sie die Variable ComputerName in Ihrer sysprep.inf- oder unattended.txt-Datei, um das neue Gerät eindeutig festzulegen, wie im nachstehenden Codebeispiel gezeigt.

```
[BenutzerDaten]
Produktschlüssel=%ProductKey%
FullName="Engineering"
OrganisationsName="LANDesk"
ComputerName=%ComputerName%
```

Verwandte Themen

"Versorgung mit Vorlagenvariablen" auf Seite 461

"Definieren einer öffentlichen (globalen) Variablen" auf Seite 463

Einbezogene Vorlagen

In der Vorlagenansicht sehen Sie die Vorlagen, die in der aktuellen Vorlage enthalten sind (einbezogene Vorlagen werden auch als untergeordnete Vorlagen bezeichnet). Sie können die einbezogenen Vorlagen anzeigen und der aktuellen Vorlage weitere Vorlagen hinzufügen. Nachdem eine Vorlage in eine Vorlage einbezogen wurde, ist sie Teil der übergeordneten Vorlage. Wenn Sie die einbezogene Vorlage in ihrem ursprünglichen eigenständigen Format ändern, wird sie im Paket der übergeordneten Vorlage ebenfalls geändert.

Um eine Vorlage einzufügen, müssen ihre Bootumgebung und das Zielbetriebssystem mit der Vorlageneinstellung der übergeordneten Vorlage übereinstimmen.

So fügen Sie der aktuellen Vorlage eine Vorlage hinzu

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf **Öffentlich** oder auf **Eigene Vorlagen**, um Vorlagen anzuzeigen.
3. Doppelklicken Sie auf eine Vorlage.
4. Klicken Sie in der Vorlagenansicht auf **Enthält**.
5. Klicken Sie auf die Schaltfläche **Einschließen**.
6. Steuern Sie mithilfe des Baumstruktur zu der Vorlage, die Sie einbeziehen möchten, wählen Sie sie aus und klicken Sie auf **OK**.

Der Abschnitt **Vorlageinformationen** zeigt Details zur Vorlage an, die unter Umstände hilfreich bei der Entscheidung sind, ob die Vorlage eingeschlossen werden soll.

Um eine Vorlage aus der Liste der eingeschlossenen Vorlagen zu löschen, klicken Sie auf **Entfernen**, um die ausgewählten Vorlagen zu löschen.

"Nicht zutreffend" wird wie ein Platzhalter behandelt.

Übergeordnete Vorlagen

Die Ansicht **Einbezogen von** blendet eine Liste anderer Vorlagen ein, in denen die aktuelle Vorlage enthalten ist (Vorlagen, in denen die aktuelle Vorlage enthalten ist, werden auch als "übergeordnete Vorlagen" bezeichnet).

So zeigen Sie die Liste der Vorlagen an, in denen die aktuelle Vorlage enthalten ist

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf **Öffentlich** oder auf **Eigene Vorlagen**, um Vorlagen anzuzeigen.
3. Doppelklicken Sie auf eine Vorlage.
4. Klicken Sie auf **Einbezogen von**.

Hinzufügen von Aktionen zu einer Versorgungsvorlage

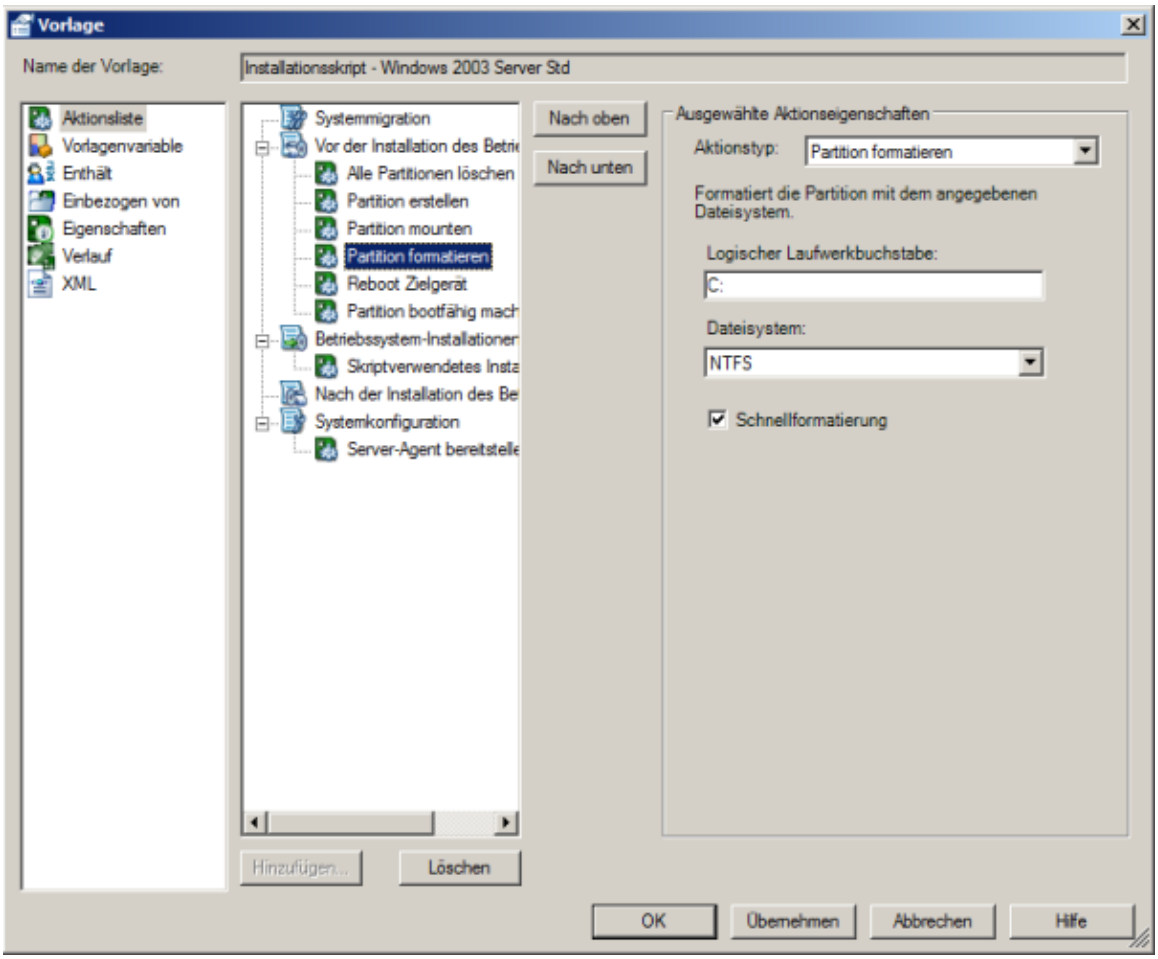
Das Dialogfeld **Aktion hinzufügen** verwenden Sie zur Erstellung neuer Aktionen für Versorgungsvorlagen oder zur Bearbeitung von Aktionen in vorhandenen Vorlagen. Öffentliche Vorlagen sind für alle Benutzer sichtbar. Dagegen können Vorlagen in der Gruppe **Eigene Vorlagen** nicht von allen Benutzern angezeigt werden. Diese Vorlagen können zudem nur vom Ersteller der Vorlage oder von Benutzern mit administrativen Rechten geändert werden.

Aktionen sind in fünf Abschnitten angeordnet. Sie können in den jeweiligen Abschnitten nur Aktionen auswählen, die auf den Abschnitt übertragen werden können (so können Sie beispielsweise "Softwareverteilung" nicht als eine Aktion für den Abschnitt "Vor der Installation..." auswählen). Sie können jede verfügbare Aktion jedem Abschnitt hinzufügen. Beachten Sie jedoch, dass einige Aktionen, wenn sie mit den falschen Schritten ausgeführten werden, die Funktionsfähigkeit der Vorlage kompromittieren oder Ihr System unbrauchbar machen können.

Die Schaltfläche **Komprimieren** veranlasst, dass alle eingeschlossenen Vorlagen sofort in die aktuelle übergeordnete Vorlage übernommen werden. Auf diese Weise werden alle Aktionen aus den einbezogenen Vorlagen Teil der übergeordneten Vorlage. Das heißt, die übergeordnete Vorlage verfügt über keine Abhängigkeiten mehr. Dies ist insbesondere für das Exportieren oder Veröffentlichen von Vorlagen nützlich. Nachdem die Vorlage komprimiert wurde, gilt sie als neue Vorlage. Eine komprimierte Vorlage kann nicht erweitert werden.

So fügen Sie einer Vorlage Aktionen hinzu

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter **Versorgungsvorlagen** auf **Öffentlich** oder auf **Eigene Vorlagen**, um Vorlagen anzuzeigen.
3. Doppelklicken Sie auf eine Vorlage.



4. Klicken Sie in der Vorlagenansicht auf **Aktionsliste**.
5. Klicken Sie auf den Abschnitt, dem Sie eine Aktion hinzufügen möchten. Folgende Abschnitte stehen zur Auswahl:

   - **Systemmigration:** Funktionen und Komponenten, die vor Systemänderungen gespeichert werden müssen (oder vor dem Migrieren eines Geräts auf eine andere Hardware oder ein virtuelles Gerät). Dieser Abschnitt kann beispielsweise eine Aktion zur Erfassung von Profilinformationen bei der Migration zu Windows Vista enthalten.
   - **Vor der Installation des Betriebssystems:** Aktionen, die durchgeführt werden, wenn das Gerät in eine Vorinstallationsumgebung (Windows PE) gebootet wird. Bei einem Server würden Sie beispielsweise in diesem Abschnitt die RAID-Konfiguration hinzufügen.
   - **Betriebssystem-Installation** Aktionen, die in der Vorinstallationsumgebung (Windows PE) bei der Installation des Betriebssystems ausgeführt werden.
   - **Nach der Installation des Betriebssystems:** Aktionen, die nach der Betriebssysteminstallation im Zielbetriebssystem durchgeführt werden, wie beispielsweise die Durchführung eines Patchmanagement-Tasks.

- **Systemkonfiguration:** Installation/Ausführung zusätzlicher Anwendungen und Systemkonfiguration im installierten Betriebssystem. Beispielsweise die Treiberinstallationstasks in diesem Abschnitt.

6. Klicken Sie auf **Hinzufügen**.
7. Geben Sie einen spezifischen Namen für die Aktion in das Feld **Name** ein.
8. Geben Sie eine detaillierte Beschreibung der Aktion in das Feld **Beschreibung** ein.
9. Wählen Sie einen Aktionstyp aus der Liste **Typ** aus. Der von Ihnen ausgewählte Typ entscheidet darüber, welche Optionen Sie für die Aktion angeben müssen.
10. Klicken Sie unter **Aktionsvariablen** auf **Hinzufügen**, um eine Variable hinzuzufügen, die nur für diese Aktion gilt. Geben Sie den Namen und Wert der Variable in die Textfelder ein und klicken Sie auf **Speichern**.
11. Markieren Sie **Das Bearbeiten der Vorlage einstellen, wenn diese Aktion fehlschlägt**, wenn Sie diese Aktion als unerlässlich für den Versorgungstask definieren wollen. Wenn die Aktion ignoriert werden kann, heben Sie die Markierung dieses Kontrollkästchens auf.
12. Wenn Sie fertig sind, klicken Sie auf **OK**.

Aktionstypen von Versorgungsvorlagen

Die Tabelle unten zeigt die Aktionstypen an und gibt Auskunft darüber, wo sie standardmäßig in den Abschnitten eingepasst werden. Sie können jeden Aktionstyp jedem Abschnitt hinzufügen. Beachten Sie jedoch, dass einige Aktionen ihrer Funktion gemäß nur in bestimmte Abfolgen passen. Wenn eine Aktion nicht in der vorgesehenen Abfolge ausgeführt wird, sind unabsehbare Fehler die Folge.

Aktionsname	Sys-temmigration	Vor der Installation des Betriebssys-tems	Betriebssystem-Installation	Nach der Installation des Betriebssys-tems	Sys-temkonfiguration
Abbild erfassen			X		
Profilerfassung	X				
Agent konfigurieren					X
Ziel-betriebssystem konfigurieren				X	
Steuerungsdienst					X
Datei kopieren	X	X	X	X	X
Verzeichnis erstellen	X	X	X	X	X
Datei löschen	X	X	X	X	X
Abbild bereitstellen			X		

Aktionsname	Sys-temmigration	Vor der Installation des Betriebssys-tems	Betriebssystem-Installation	Nach der Installation des Betriebssys-tems	Sys-temkonfiguration
Pro-filbereitstellung					X
Software verteilen					X
Datei downloaden	X	X	X	X	X
Download vom bevorzugten Server	X	X	X	X	X
Datei ausführen	X	X	X	X	X
Hard-ware-unabhängige Abbilderstellung				X	
Skript injizieren	X	X	X	X	X
Dienst installieren					X
Einer Domäne beitreten					X
Laufwerk zuord-nen/Zuordnung aufheben	X	X	X	X	X
Laufwerk dem bevorzugten Server zuord-nen/Zuordnung aufheben	X	X	X	X	X
Partition		X	X	X	
System patchen					X
Neu starten/He-runterfahren	X	X	X	X	X
Text ersetzen	X	X	X	X	X
Skriptgesteuerte			X		

Aktionsname	Sys-temmigration	Vor der Installation des Betriebssys-tems	Betriebssystem-Installation	Nach der Installation des Betriebssys-tems	Sys-temkonfiguration
Installation					
Dienst deinstallieren					X
Datei entpacken	X	X	X	X	X
Registrierung aktualisieren					X
Warten	X	X	X	X	X

Abbild erfassen (nur Abschnitt "Betriebssystem-Installation")

Mit der Aktion "Abbild erfassen" können Sie während der Installation des Betriebssystems mithilfe des von Ihnen angegebenen Abbilderstellungstools ein Abbild aufzeichnen. Wenn das Tool oder der in einem Abbild zu erfassende Inhalt sich auf derselben Freigabe befindet, müssen Sie der Aktion "Abbild erfassen" die Aktion "Laufwerk zuordnen" voranstellen, um eine Authentifizierung gegenüber der Freigabe zu ermöglichen.

- **Abbildtyp auswählen:** Wählen Sie den Abbildtyp aus, den Sie erfassen möchten. Wenn Sie "Symantec" oder "Sonstige" auswählen, müssen Sie auch einen Pfad zu der Anwendung für die Abbilderstellung angeben.
- **Geben Sie den UNC-Pfad zur Abbilddatei ein:** Geben Sie einen UNC-Pfad zu dem Abbild ein, das erfasst wird, sowie den Namen der Abbilddatei. Konfigurieren Sie Ihren bevorzugten Server mit gültigen Anmeldeinformationen für die Freigabe mit dem Pfad zur Abbilddatei. Diese Option wird verwendet, wenn Sie als Abbildtyp "LANDesk ImageW" oder "ImageX" auswählen.
- **Geben Sie den zugeordneten Laufwerkspfad zur Abbilddatei ein:** Geben Sie einen Pfad zur Abbilddatei ein, einschließlich dem Laufwerksbuchstaben und dem Namen der Abbilddatei. Diese Option wird verwendet, wenn Sie als Abbildtyp "Symantec" oder "Sonstige" auswählen.
- **Geben Sie den zugeordneten Laufwerkspfad zum Abbilderstellungstool ein:** Geben Sie einen zugeordneten Laufwerkspfad und einen Dateinamen für die Anwendung zur Abbilderstellung ein. Diese Option wird verwendet, wenn Sie als Abbildtyp "Symantec" oder "Sonstige" auswählen.
- **Befehlszeilenparameter:** Geben Sie einen beliebigen Befehlszeilenparameter an, mit dem die zur Erfassung des Abbilds verwendete Methode angepasst wird.
- **Validieren:** Klicken Sie auf diese Schaltfläche, um eine Standardbefehlszeile für das von Ihnen angegebene Abbilderstellungstool und den von Ihnen angegebenen Pfad zu generieren. Sie können weitere Befehlszeilenparameter hinzufügen, nachdem Sie auf "Validieren" geklickt haben. Wenn Sie jedoch bereits benutzerdefinierte Parameter eingegeben hatten, werden diese beim Klicken auf "Validieren" entfernt.

HINWEIS: Um zu vermeiden, dass das Dateisystem in WinPE entsperrt wird, müssen Sie Ihr Abbild zuerst mit Sysprep vorbereiten. Befolgen Sie die nachstehenden Schritte in Windows Vista.

1. Starten Sie Vista.
2. Wechseln Sie in das Verzeichnis %SystemRoot%\System32\sysprep
3. Führen Sie "sysprep /generalize /shutdown" aus.
4. Starten Sie PE und führen Sie ImageX aus.

Die Schritte in Windows XP/2003 machen die Switches "/generalize" und "/shutdown" für sysprep nicht erforderlich. Der Programmschalter "/factory" sollte auf diesen Betriebssystemen funktionieren.

Profil erfassen (nur Abschnitt "Systemmigration")

Diese Aktion führt den Benutzermigrations-Assistenten zur Erfassung von einem oder mehreren Profilen aus. Wenn Sie diese Aktion verwenden möchten, müssen Sie den Speicherort der XML-Befehlsdatei des Benutzermigrations-Assistenten auf dem Coreserver kennen und wissen, wo gespeicherte Profile abzulegen sind.

Sie können eindeutige Bezeichner für die Benennung von Profilen beim Speichern verwenden oder aber einen vollständigen Dateinamen für das Profil angeben.

Damit der Benutzermigrations-Assistent eingesetzt werden kann, müssen auf den verwalteten Geräten der Standard LANDesk Agent, der den Inventarscanner und Local Scheduler umfasst, und der Softwareverteilungsagent installiert sein. Die Profilmigration verwendet den Softwareverteilungsagenten, um Dateien zu verteilen.

- **XML-Befehlsdatei des Benutzermigrations-Assistenten auswählen:** Geben Sie den Speicherort der Befehlsdatei des Benutzermigrations-Assistenten an. Hierbei handelt es sich um eine XML-Datei, die auf dem Coreserver (normalerweise in der ldmain-Freigabe im Ordner ldlogon\uma\commandxml) gespeichert ist. Sie können den Pfad und den Dateinamen im UNC- oder HTTP-Format angeben. Klicken Sie auf **Durchsuchen**, um die Befehlsdatei anzusteuern, die Sie verwenden möchten. Wenn Sie eine vorhandene Befehlsdatei bearbeiten oder eine neue Befehlsdatei erstellen möchten, klicken Sie auf **Bearbeiten**. Wählen Sie eine Datei aus und klicken Sie auf **Bearbeiten** oder klicken Sie auf **Neu**, um eine neue Datei zu erstellen.
- **UNC-Pfad für gespeicherte Profile:** Geben Sie an, wo die Profildateien gespeichert werden sollen. Geben Sie einen UNC-Pfad ein oder klicken Sie auf **Durchsuchen** und wählen Sie einen Pfad aus. Profile können auf jedem verfügbaren Server bzw. jeder verfügbaren Freigabe gespeichert werden, auch auf dem Coreserver. Profile werden mit der Erweiterung .sma gespeichert.
- **Keine Variablen, sondern vollständigen Dateinamen eingeben:** Markieren Sie dieses Kontrollkästchen, wenn Sie zur Benennung des Profils keine eindeutigen Bezeichner verwenden möchten.
- **Eindeutige Bezeichner für Dateinamen:** Wählen Sie eine beliebige Kombination aus Computername, MAC-Adresse und Seriennummer für die Erstellung eines Dateinamens für die einzelnen Profile. (Wenn Sie beispielsweise **Seriennummer** wählen und die Seriennummer des Geräts lautet 1234567B, dann wird der Profilname als "1234567B.sma" gespeichert.)

Agent konfigurieren (nur Abschnitt "Systemkonfiguration")

Mithilfe der Aktion "Agent konfigurieren" können Sie auf dem zu versorgenden Gerät eine Agentenkonfiguration installieren. Dies sollte die erste Aktion sein, die Sie nach dem auf die Aktion "Betriebssysteminstallation" folgenden Neustart ausführen. Konfigurationen werden während ihrer Erstellung im Dialogfeld "Agentenkonfiguration" der Dropdownliste hinzugefügt. Diese Aktion kann nur als Teil einer Vorlage ausgeführt werden, die entweder die Aktion zur skriptgesteuerten Installation oder zur Abbildbereitstellung einschließt, oder wenn der Clientcomputer bereits mit einem Agenten konfiguriert wurde.

- **Konfigurationsname:** Der Name der Konfiguration. Wählen Sie eine Konfiguration aus der Liste mit den gültigen Agentenkonfigurationen aus.
- **Anmeldeinformationen:** Geben Sie den Domänen- und Benutzernamen für die Anmeldung bei dem Coreserver ein, auf dem sich die Agentenkonfiguration befindet.
- **Variable als Kennwort verwenden:** Markieren Sie dieses Kontrollkästchen, um eine Variable für das Kennwort zu verwenden. Diese Variable wird in den **Vorlagenvariablen** unter dem Datentyp **Private Daten** definiert. Geben Sie den Variablennamen in Prozentzeichen eingeschlossen (%Variablenname%) in das Feld **Kennwort** ein. Weitere Informationen finden Sie unter "Definieren einer Vorlagenvariablen" auf Seite 464.
- **Kennwort:** Geben Sie das Kennwort für die Anmeldung beim Coreserver ein. Bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.
- **Neu starten, falls erforderlich:** Markieren Sie dieses Kontrollkästchen, um einen Neustart des Geräts im Anschluss an die Agentenkonfiguration zuzulassen, falls ein Neustart erforderlich ist.

Beim Installieren eines neuen Service Packs ändern sich die Datenbankkennungen der Agentenkonfiguration. Das bedeutet, dass die Vorlagen, die auf diese Konfigurationen verweisen, ungültig werden. Aus diesem Grund ist der Versorgungsverlauf, der auf diese Konfigurationen verweist, nicht in der Lage, den Namen der Konfiguration anzuzeigen, auf die er vormals verwies. Alle Vorlagen, die auf die alten Konfigurationen verweisen, müssen deshalb aktualisiert werden, da sie andernfalls nicht ordnungsgemäß ausgeführt werden. Der Konfigurationsname wird nicht auf der Seite "Verlauf" angezeigt, und wenn Sie versuchen, diese Vorlage erneut einzuplanen, schlägt sie während der Agentenkonfigurationsaktion fehl. Um dieses Problem zu beheben, müssen Sie die Vorlage duplizieren, die duplizierte Vorlage sowie die Aktion "Agentenkonfiguration" öffnen und dann die Konfiguration zuweisen, die Sie verwenden möchten. Danach wird der Task erfolgreich ausgeführt.

Zielbetriebssystem konfigurieren (nur Abschnitt "Nach der Installation des Betriebssystems")

Diese Aktion setzt den Versorgungsagenten (ldprovision) in ein Abbild ein, damit der Agent nach dem Neustart installiert werden kann. Dieser Agent wird für die fortgesetzte Versorgung nach dem Start des neuen Betriebssystems benötigt. Damit die Aktion ausgeführt wird, müssen folgende Bedingungen erfüllt sein:

1. Das Windows-Systemlaufwerk muss bereitgestellt worden sein.
2. Das Windows-Dateisystem muss entweder mit Sysprep vorbereitet worden sein oder einen Agenten auf dem Computer installiert haben.
3. Linux darf keine unbekannten Dateisysteme (xfs, jfs, bobfs) aufweisen. Die Betriebssysteme "reiserfs" und "ext2/3" sind derzeit die einzig unterstützten Betriebssysteme.

4. Das Linux-Rootsystem darf sich nicht auf einem Software-RAID-Controller oder auf einem Software-RAID (md's) befinden. Echte Hardware-RAID-Konfigurationen sind zulässig, solange PE den Controllertreiber erkennt.

- **Eindeutige Kennung eingeben:** Um die vorhandene Gerätekennung zu verwenden, markieren Sie dieses Kontrollkästchen und geben die Gerätekennung in das Feld ein.

Diese Aktion sollte als letzte im Abschnitt "nach der Installation des Betriebssystems" durchgeführt werden, weil sie eine Neustartoperation enthält.

Steuerungsdienst (nur Abschnitt "Systemkonfiguration")

Die Aktion "Steuerungsdienst" startet oder beendet einen spezifischen Dienst oder startet ihn neu. Das Zielbetriebssystem für diese Aktion muss Windows sein.

- **Dienstname:** Der Anzeigename des Dienstes.
- **Dienststeuerungsaktion:** Die auf dem Dienst auszuführende Aktion. Die Optionen lauten "Stopp", "Start" oder "Neustart".

Datei kopieren (alle Abschnitte)

Mit der Aktion "Datei kopieren" werden Dateien in spezifische Speicherorte auf dem Zielgerät kopiert. Sowohl Quelle als auch Ziel können sich auf der Freigabe befinden. Ist dies der Fall, so müssen Sie der Aktion "Datei kopieren" eine Aktion "Laufwerk zuordnen" voranstellen. Die Aktion "Datei kopieren" kann wiederholt auftreten, d. h. alle Dateien/Ordner unterhalb des Quellenpfads können kopiert werden und behalten dabei ihre Originalstruktur. Platzhalterzeichen werden unterstützt (z. B. *.exe oder ld*.*).

- **Quellpfad und Dateiname:** Der Server-/Freigabepfad und Dateiname der zu kopierenden Datei. Wenn Sie alle Dateien und Ordner unterhalb des Quellenpfads kopieren möchten, ist kein Dateiname nötig.
- **Zielpfad und Dateiname:** Der Server-/Freigabepfad und Dateiname, in den die Datei kopiert werden soll.
- **Unterverzeichnisse kopieren:** Kopiert alle Unterordner und Dateien unterhalb der Quelle.

Verzeichnis erstellen (alle Abschnitte)

Die Aktion "Verzeichnis erstellen" erstellt ein Verzeichnis am angegebenen Speicherort und kann ggf. ein übergeordnetes Verzeichnis anlegen.

- **Verzeichnispfad:** Geben Sie den Pfad für das zu erstellende Verzeichnis ein.
- **Erstellen Sie ggf. ein übergeordnetes Verzeichnis:** Wählen Sie dieses Kontrollkästchen zum Erstellen des übergeordneten Verzeichnisses aus.

Datei löschen (alle Abschnitte)

Mit der Aktion "Datei löschen" werden Dateien aus spezifischen Speicherorten auf dem Zielserver entfernt. Der Pfad kann sich auf einer Freigabe befinden. Ist dies der Fall, so müssen Sie der Aktion "Datei löschen" die Aktion "Laufwerk zuordnen" voranstellen. Die Aktion "Datei löschen" kann wiederholt auftreten, d. h. alle Dateien/Ordner unter dem Quellenpfad können gelöscht werden. Platzhalterzeichen werden unterstützt (z. B. *.exe oder ld*.*).

- **Pfad und Dateiname:** Geben Sie den vollständigen Pfad und Namen der zu löschenden Datei ein.
- **Subverzeichnisse löschen:** Löscht alle Unterordner und -dateien unterhalb der Quelle.

Abbild bereitstellen (nur Abschnitt "Betriebssystem-Installation")

Mit dieser Aktion wird das ausgewählte Abbild mithilfe des von Ihnen angegebenen Abbilderstellungstools auf dem Zielserver bereitgestellt. Wenn sich das Tool oder das bereitzustellende Abbild auf derselben Freigabe befindet, müssen Sie der Aktion "Abbild bereitstellen" die Aktion "Laufwerk zuordnen" voranstellen, um eine Authentifizierung gegenüber der Freigabe zu ermöglichen.

Nach der Bereitstellung eines Abbilds müssen Sie einen manuellen Neustart ausführen.

- **Abbildtyp auswählen:** Wählen Sie den Abbildtyp aus, den Sie bereitstellen möchten. Wenn Sie "Symantec" oder "Sonstige" auswählen, müssen Sie auch einen Pfad zu der Anwendung für die Abbilderstellung angeben.
- **Geben Sie den UNC-Pfad zur Abbilddatei ein:** Geben Sie einen UNC-Pfad zu dem Abbild ein, das bereitgestellt wird, sowie den Namen der Abbilddatei. Konfigurieren Sie Ihren bevorzugten Server mit gültigen Anmeldeinformationen für die Freigabe mit dem Pfad zur Abbilddatei. Diese Option wird verwendet, wenn Sie als Abbildtyp "LANDesk ImageW" oder "ImageX" auswählen.
- **Geben Sie den zugeordneten Laufwerkspfad zur Abbilddatei ein:** Geben Sie einen Pfad zum Abbild ein, einschließlich dem Laufwerksbuchstaben und dem Namen der Abbilddatei. Diese Option wird verwendet, wenn Sie als Abbildtyp "Symantec" oder "Sonstige" auswählen.
- **Geben Sie den zugeordneten Laufwerkspfad zum Abbilderstellungstool ein:** Geben Sie einen zugeordneten Laufwerkspfad und einen Dateinamen für die Anwendung zur Abbilderstellung ein. Diese Option wird verwendet, wenn Sie als Abbildtyp "Symantec" oder "Sonstige" auswählen.
- **Befehlszeilenparameter:** Geben Sie einen beliebigen Befehlszeilenparameter an, mit dem die zur Bereitstellung des Abbilds verwendete Methode angepasst wird.
- **Validieren:** Klicken Sie auf diese Schaltfläche, um eine Standardbefehlszeile für das von Ihnen angegebene Abbilderstellungstool und den von Ihnen angegebenen Pfad zu generieren. Sie können weitere Befehlszeilenparameter hinzufügen, nachdem Sie auf "Validieren" geklickt haben. Wenn Sie jedoch bereits benutzerdefinierte Parameter eingegeben hatten, werden diese beim Klicken auf "Validieren" entfernt.

Profil bereitstellen (nur Abschnitt "Systemkonfiguration")

Diese Aktion führt den Benutzermigrations-Assistenten aus, um ein oder mehrere Profile bereitzustellen, die erfasst und gespeichert wurden. Um diese Aktion einsetzen zu können, müssen Sie wissen, an welchem Speicherort die Profile gespeichert wurden.

Damit der Benutzermigrations-Assistent eingesetzt werden kann, müssen auf den verwalteten Geräten der Standard LANDesk Agent, der den Inventarscanner und Local Scheduler umfasst, und der Softwareverteilungsagent installiert sein. Die Profilmigration verwendet den Softwareverteilungsagenten, um Dateien zu verteilen.

- **UNC-Pfad, in dem das Profil zuvor gespeichert wurde:** Geben Sie an, wo die Profildateien gespeichert werden. Geben Sie einen UNC-Pfad ein oder klicken Sie auf **Durchsuchen** und wählen Sie einen Pfad aus. Profile können auf jedem verfügbaren Server bzw. jeder verfügbaren Freigabe gespeichert werden, auch auf dem Coreserver. Profile werden mit der Erweiterung .sma gespeichert.
- **Keine Variablen, sondern vollständigen Dateinamen eingeben:** Markieren Sie dieses Kontrollkästchen, wenn Sie zur Benennung des Profils keine eindeutigen Bezeichner verwenden möchten.

- **Eindeutige Bezeichner für Dateinamen:** Wählen Sie eine beliebige Kombination aus Computername, MAC-Adresse und Seriennummer für die Erstellung eines Dateinamens für die einzelnen Profile. (Wenn Sie beispielsweise **Seriennummer** wählen und die Seriennummer des Geräts lautet 1234567B, dann wird der Profilname als "1234567B.sma" gespeichert.)

Software verteilen (nur Abschnitt "Systemkonfiguration")

Diese Aktion verteilt ein Softwareverteilungspaket an das Ziel. Sie können ein beliebiges Verteilungspaket auswählen, das Sie im Extra "Verteilungspakete" gespeichert haben. Diese Aktion kann nur im Anschluss an die Agentenkonfiguration durchgeführt werden oder nachdem Agenten auf dem Gerät installiert wurden.

- **Softwareverteilungspaket:** Wählen Sie das zu verteilende Paket aus.

Datei downloaden (alle Abschnitte)

Mit der Aktion "Datei downloaden" wird die ausgewählte Datei mithilfe eines anonymen Benutzers (anonyme HTTP-Anmeldung) auf ein von Ihnen angegebenes Ziel heruntergeladen. Wenn die sich Downloaddateien oder das Ziel auf derselben Freigabe befinden, müssen Sie der Aktion "Datei downloaden" die Aktion "Laufwerk zuordnen" voranstellen, um eine Authentifizierung gegenüber der Freigabe zu ermöglichen.

- **Quellpfad und Dateiname:** Der aktuelle Server-/Freigabepfad und Name der Datei, die heruntergeladen werden soll. Das Downloaden von Dateien von einem UNC-Pfad wird nicht unterstützt. Wenn Sie eine Datei von einem UNC-Pfad downloaden möchten, sollten Sie die Aktion "Laufwerk zuordnen" zur Herstellung einer Zuordnung zum UNC-Pfad verwenden und anschließend die Aktion "Datei kopieren".
- **Zielpfad und Dateiname:** Der Speicherort, an den die Datei heruntergeladen werden soll.
- **Proxyserver verwenden:** Aktiviert die Proxyserver-Option zum Downloaden einer Datei. Standardmäßig ist diese Option deaktiviert. Wenn Sie einen Proxyserver aktivieren, müssen Sie die Adresse und den Port in die unten stehenden Felder eingeben.
- **Adresse:** Gibt die IP-Adresse Ihres Proxyservers an.
- **Port:** Gibt die Portnummer Ihres Proxyservers an.
- **Erfordert Anmeldung:** Ermöglicht die Eingabe eines Benutzernamens und eines Kennworts, wenn der Proxyserver Anmeldeinformationen verlangt und kein transparenter Proxyserver ist.
    - **Benutzername:** Geben Sie einen gültigen Benutzernamen und Anmeldeinformationen für die Authentifizierung gegenüber dem Proxyserver ein.
    - **Variable als Kennwort verwenden:** Markieren Sie dieses Kontrollkästchen, um eine Variable für das Kennwort zu verwenden. Diese Variable wird in den **Vorlagenvariablen** unter dem Datentyp **Private Daten** definiert. Geben Sie den Variablennamen in Prozentzeichen eingeschlossen (%Variablenname%) in das Feld **Kennwort** ein. Weitere Informationen finden Sie unter "Definieren einer Vorlagenvariablen" auf Seite 464.
    - **Kennwort:** Geben Sie das Kennwort des Benutzers ein. Bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.

Download vom bevorzugten Server (alle Abschnitte)

Diese Aktion verwendet Inhaltsreplikation für den Datendownload von einem bevorzugten Server auf das Zielgerät. Der Download kann eine einzelne Datei oder den Inhalt eines ganzen Ordners (mit Unterordnern) auf dem Quellserver umfassen. Damit Sie diese Option verwenden können, müssen Sie mindestens einen bevorzugten Server unter Verwendung des Extras "Inhaltsreplikation" konfiguriert haben. Welcher bevorzugte Server schließlich verwendet wird, hängt von den Einstellungen an, die Sie bei der Einrichtung der bevorzugten Server im Extra "Inhaltsreplikation" definiert haben.

- **Quelle**: Geben Sie den Pfad zu der Datei oder zu dem Ordner an, die bzw. den Sie herunterladen möchten. Dieser Pfad muss auf allen Freigaben vorhanden sein, die für Downloads von bevorzugten Servern verwendet werden.
- **Downloadverzeichnis:** Markieren Sie dieses Kontrollkästchen, um den gesamten Ordner herunterzuladen, der Im Feld **Quelle** angegeben ist. Ist dieses Kästchen nicht markiert, wird nur die von Ihnen angegebene Datei heruntergeladen.
- **Ziel:** Geben Sie den Pfad auf dem Zielgerät ein, in den Sie die Datei oder den Ordner kopieren möchten.
- **Bevorzugte Downloadspeicherorte:** Mit den drei Kontrollkästchen können Sie angeben, welche Downloadquellen Sie verwenden möchten. Diese sind nach Priorität geordnet: Wenn alle drei Kästchen aktiviert werden, wird zunächst ein Peerdownload versucht, anschließend ein Download von einem bevorzugten Server und schließlich ein Download von der Quelle.
    - **Peer versuchen:** Markieren Sie dieses Kontrollkästchen, wenn zuerst ein Download vom Peer versucht werden soll. Der Replikator prüft zunächst lokale Peers auf Quelldateien, die repliziert werden sollen. Wenn der Replikator die Dateien nicht auf einem Peer finden kann, versucht er die Dateien von einem bevorzugten Server oder vom Quellserver herunterzuladen. Diese Option kann dazu beitragen, den Datenverkehr auf den bevorzugten Servern und auf Ihrem Quellserver zu reduzieren.
    - **Bevorzugten Server versuchen:** Markieren Sie dieses Kontrollkästchen, wenn der Download von einem bevorzugten Server versucht werden soll. Wenn der Replikator die Dateien nicht auf einem bevorzugten Server finden kann, versucht er die Dateien vom Quellserver herunterzuladen.
    - **Quelle zulassen:** Markieren Sie dieses Kontrollkästchen, wenn der Download von der Dateiquelle erfolgen soll. Dies empfiehlt sich nur als zweite Option, wenn ein Download vom Peer oder bevorzugten Server nicht durchgeführt werden kann.
- **Vom Core oder bevorzugten Server genutzte Bandbreite:** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. WAN-Verbindungen sind in der Regel langsamer, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen niedrigeren Prozentsatz einzustellen.
- **Von Peer zu Peer genutzte Bandbreite:** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. LAN-Verbindungen sind in der Regel schneller als WAN-Verbindungen, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen höheren Prozentsatz einzustellen, als den Prozentsatz für WAN.

Datei ausführen (alle Abschnitte)

Die Aktion "Datei ausführen" führt die ausgewählte Datei auf dem Zielserver gemeinsam mit etwaigen Befehlszeilenparametern oder Rückgabecodes aus, die Sie angeben.

- **Zielpfad und Dateiname:** Der Speicherort der auszuführenden Datei.
- **Befehlszeilenparameter:** Geben Sie beliebige Befehlszeilenparameter an, mit denen die Ausführungsmethode für die Datei angepasst wird.
- **Arbeitsverzeichnis:** Das Programm wird mit Hinweis auf dieses Verzeichnis ausgeführt. Alle unterstützenden Dateien des Programms sollten sich in diesem Verzeichnis befinden. Die Befehlszeilenparameter starten von diesem Referenzpunkt aus.
- **Erwarteter Rückgabewert:** Der erwartete Wert, der von der Anwendung bei der Ausführung zurückgegeben wird. Zulässige Werte sind "Beliebig", "Ist gleich (=)", "Kleiner als (<)", "Größer als (>)" oder "Zwischen". Wenn der Wert jedem Wert außer "Beliebig" entsprechen soll, geben Sie die erwarteten Werte in die bereitgestellten Felder ein.
- **Einfügen:** Öffnet das Dialogfeld **Umgebungsvariable**, in dem Sie eine Umgebungsvariable und den zugehörigen Wert eingeben können.
    - **Name:** Geben Sie den Namen der Umgebungsvariablen der Datei ein. Verwenden Sie doppelte Prozentzeichen zur Angabe von Umgebungsvariablen (zum Beispiel: %%windir%%\system32\calc.exe).
    - **Wert:** Geben Sie den Wert der Variable ein.
- **Ändern:** Ändern Sie die ausgewählte Variable.
- **Entfernen:** Löschen Sie die ausgewählte Variable.
- **Befehlsausgabe erfassen:** Bei Aktivierung dieses Kontrollkästchens wird die Ausgabe der ausführbaren Datei in eine Protokolldatei geschrieben. Heben Sie die Markierung dieses Kontrollkästchens auf, wenn die Ausgabe nicht erfasst werden soll.

Hardwareunabhängige Abbilderstellung (nur nach der Installation des Betriebssystems)

Die Aktion "Hardwareunabhängige Abbilderstellung" schließt das Extra "Hardwareunabhängige Abbilderstellung" (hiiclient.exe) im Versorgungsprozess ein. Mit der hardwareunabhängige Abbilderstellung (HII, Hardware-independent imaging) können Sie ein einziges Repository mit Gerätetreibern erstellen, dass in Versorgungsvorlagen oder Bereitstellungsskripts injiziert werden kann. Auf dem Gerät wird zunächst ein Basisabbild installiert, und das HII-Extra injiziert dann die für dieses Gerätemodell spezifischen Treiber.

Diese Aktion ist nur im Abschnitt "Nach der Installation des Betriebssystems" für Vorlagen enthalten, die auf der Windows-Prebootumgebung basieren. Nach der Installation des Betriebssystems, aber noch vor dem Neustart des Geräts, erkennt das HII-Extra das Gerätemodell und ruft Treiber für dieses Modell ab. Die Treiber werden auf dem Gerät installiert und die zugehörigen Information werden in die Registry aufgenommen. Wenn das Betriebssystem dann nach einen Neustart hochfährt, werden die Treiber konfiguriert.

- **UNC zum Kopieren von Treiberdateien verwenden:** Markieren Sie dieses Kontrollkästchen, um anzugeben, dass für den Zugriff auf das HII-Repository nur UNC verwendet werden soll.

Wenn Sie diese Aktion verwenden, sollten Sie im Anschluss daran eine Neustartaktion in den Abschnitt "Nach der Installation des Betriebssystems" einschließen.

Skript injizieren (alle Abschnitte)

Diese Aktion injiziert ein Skript in das Dateisystem des Zielbetriebssystems. Sie können beispielsweise sysprep.inf in die Aktion "Abbild bereitstellen" oder unattend.txt in eine Aktion des Typs "skriptgesteuerte Installation" injizieren. Auf die aktuelle Vorlage können Sie die Skripte anwenden, die in der Auswahlliste **Installationsskripte** der Vorlage aufgeführt sind. Der Zugriff auf diese Liste erfolgt über die Schaltfläche **Installationskripte** der Symbolleiste "Versorgung".

Beim Injizieren eines Skripts wird die Datei auf den lokalen Computer kopiert und ferner werden sämtliche Variablen in der Datei ersetzt. Diese Aktion ist nützlich, wenn Sie Variablen in einer Textdatei ersetzen möchten, beispielsweise in einer Windows Sysprep-Antwortdatei.

- **Skriptname:** Der Name des Skripts.
- **Zieldateiname:** Der Speicherort des zu injizierenden Skripts.

Dienst installieren (nur Abschnitt "Systemkonfiguration")

Das Zielbetriebssystem für diese Aktion muss Windows sein.

- **Anzeigename:** Der Name, der angezeigt werden soll, um den Dienst zu repräsentieren.
- **Dienstname:** Der Name des Dienstes.
- **Dienstbeschreibung**: Eine Beschreibung des Dienstes
- **Zielpfad und Dateiname:** Der Speicherort des zu installierenden Dienstes.
- **Befehlszeilenparameter:** Geben Sie einen beliebigen Befehlszeilenparameter ein, mit dem die zur Installation des Dienstes verwendete Methode angepasst wird.
- **Dienst-Starttyp:** Die Optionen lauten "Manuell", "Automatisch" oder "Deaktiviert".
- **Interaktiver Dienst:** Wählen Sie diese Option, um auf dem Desktop eine Benutzerschnittstelle anzuzeigen, die beim Starten des Dienst vom angemeldeten Benutzer verwendet werden kann. Diese schließt alle Meldungsfelder ein, die der Dienst während des Installationsprozesses möglicherweise aktiviert. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird die Vorlage ohne Benutzereingriff ausgeführt, wobei bei jeder eingeblendeten Meldung von der Verwendung der Standardauswahl ausgegangen wird. Wenn der Dienst während des Startvorgangs irgendwelche Meldungen anzeigt, kann es sein, dass die Vorlage angehalten wird, bis das Meldungsdialogfeld wieder geschlossen wird.

Einer Domäne beitreten (nur Abschnitt "Systemkonfiguration")

Verknüpft das Zielgerät mit einer Domäne oder Arbeitsgruppe.

- **Ausgewählter Vorgangstyp:** Kann "Der Domäne beitreten" oder "Der Arbeitsgruppe beitreten" sein.
- **Domänenname:** Geben Sie die Domäne ein, der Sie beitreten möchten.
- **Arbeitsgruppenname:** Geben Sie die Arbeitsgruppe ein, der Sie beitreten möchten.
- **Benutzername:** Geben Sie den für die Authentifizierung bei der Domäne erforderlichen Benutzernamen an.
- **Variable als Kennwort verwenden:** Markieren Sie dieses Kontrollkästchen, um eine Variable für das Kennwort zu verwenden. Diese Variable wird in den **Vorlagenvariablen** unter dem Datentyp **Private Daten** definiert. Geben Sie den Variablennamen in Prozentzeichen eingeschlossen (%Variablenname%) in das Feld **Kennwort** ein. Weitere Informationen finden Sie unter "Definieren einer Vorlagenvariablen" auf Seite 464.

- **Kennwort:** Geben Sie das Kennwort ein, das dem obigen Benutzernamen entspricht. Bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.

Laufwerk zuordnen/Zuordnung aufheben (alle Abschnitte)

Diese Aktion verwenden Sie um ein Laufwerk bei Windows-Geräten zuzuordnen oder um dessen Zuordnung aufzuheben (d. h. das Laufwerk zu trennen) bzw. bei Linux-Geräten, um eine Verbindung zu einer Ressource herzustellen oder zu trennen. Beachten Sie, dass manche Systeme keine Laufwerkzuordnungen unter H: akzeptieren.

- **Laufwerk zuordnen/Zuordnung aufheben:** Wählen Sie aus, ob mit dieser Aktion ein Laufwerk zugeordnet bzw. dessen Zuordnung aufgehoben (es getrennt) werden soll oder ob eine Ressource verbunden bzw. deren Verbindung getrennt werden soll (bei Linux-Geräten).
- **UNC-Pfad:** Geben Sie den Server und die Freigabe ein, für die Sie eine Zuordnung erstellen möchten.
- **Ressourcenpfad, für den die Verbindung getrennt werden soll:** Beim Trennen einer Ressource müssen Sie den Pfad angeben, der getrennt werden soll.
- **Laufwerksbuchstabe/Bereitstellungspunkt:** Geben Sie den Laufwerksbuchstaben ein, dem Sie den Pfad zuordnen möchten. Wenn Sie sich entscheiden, die Zuordnung eines Laufwerks aufzuheben, geben Sie den Namen des Laufwerks ein, für das Sie die Verbindung aufheben möchten. Unter Linux geben Sie den Bereitstellungspunkt an, über den die Ressource oder das Dateisystem gemountet bzw. eingebunden sind.
- **Benutzername:** Geben Sie den Namen der Benutzeranmeldeinformationen ein, die für die Anmeldung beim Laufwerk benötigt werden.
- **Variable als Kennwort verwenden:** Markieren Sie dieses Kontrollkästchen, um eine Variable für das Kennwort zu verwenden. Diese Variable wird in den **Vorlagenvariablen** unter dem Datentyp **Private Daten** definiert. Geben Sie den Variablennamen in Prozentzeichen eingeschlossen (%Variablenname%) in das Feld **Kennwort** ein. Weitere Informationen finden Sie unter "Definieren einer Vorlagenvariablen" auf Seite 464.
- **Kennwort:** Geben Sie das Kennwort ein, das dem obigen Benutzernamen entspricht. Bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.

Laufwerk dem bevorzugten Server zuordnen/Zuordnung aufheben (alle Abschnitte)

Mit dieser Aktion wird ein Laufwerk auf einem Zielgerät einem Pfad auf einem bevorzugten Server (oder auf dem Quellserver) zugeordnet. Diese Laufwerkszuordnung bleibt so lange bestehen, bis die Zuordnung des Laufwerks explizit aufgehoben (es getrennt) wird, daher sollten Sie nach einer Aktion, die Daten von einem bevorzugten Server herunterlädt, ein Aktion vom Typ "Zuordnung aufheben" in die Vorlage einschließen. Damit Sie diese Option verwenden können, müssen Sie mindestens einen bevorzugten Server unter Verwendung des Extras "Inhaltsreplikation" konfiguriert haben. Welcher bevorzugte Server schließlich verwendet wird, hängt von den Einstellungen an, die Sie bei der Einrichtung der bevorzugten Server im Extra "Inhaltsreplikation" definiert haben.

- **Laufwerksbuchstabe:** Geben Sie den Laufwerksbuchstaben ein, dem Sie den Pfad zuordnen möchten. Wenn Sie sich entscheiden, die Zuordnung eines Laufwerks aufzuheben, geben Sie den Namen des Laufwerks ein, für das Sie die Verbindung aufheben möchten.
- **Laufwerkszuordnung aufheben:** Markieren Sie dieses Kontrollkästchen, wenn die Aktion in der Aufhebung der Laufwerkszuordnung bestehen soll. Die Aktion hebt die Zuordnung zu dem unter "Laufwerksbuchstabe" angegebenen Laufwerk auf bzw. trennt die Verbindung zu diesem Laufwerk.

- **Pfad:** Geben Sie den Pfad zu diesem Laufwerk im UNC-Format ein (\\Freigabename\Pfad) Dieser Pfad muss auf dem Quellserver und auf allen Freigaben vorhanden sein, die für Downloads von bevorzugten Servern verwendet werden.
- **Bevorzugten Server versuchen:** Markieren Sie dieses Kontrollkästchen, wenn zuerst versucht werden soll, das Laufwerk dem nächstgelegenen bevorzugten Server zuzuordnen, der die angegebene Ordnerstruktur aufweist. Wird kein Server gefunden, der diese Ordnerstruktur aufweist, wird der Versuch unternommen, das Laufwerk dem Pfad auf dem Quellserver zuzuordnen.
- **Bevorzugten Server verlangen:** Markieren Sie dieses Kontrollkästchen, um das Laufwerk dem nächstgelegenen bevorzugten Server zuzuordnen, der die angegebene Ordnerstruktur aufweist. Wird kein bevorzugter Server mit der Ordnerstruktur gefunden, schlägt der Task fehl (statt dass die Zuordnung zum Quellserver erfolgt).
- **Bevorzugten Server nicht zulassen:** Markieren Sie dieses Kontrollkästchen, um das Laufwerk dem Pfad auf dem Quellserver zuzuordnen, ohne eine Zuordnung zu einem bevorzugten Server vorzunehmen.

Partition (Nur Abschnitte "Vor der Installation des Betriebssystems", "Betriebssystem-Installation", "Nach der Installation des Betriebssystems")

Mit der Partitionsaktion können Sie eine Vielzahl von Aktionen bezogen auf die Partitionen auf dem Zielserver ausführen. Wählen Sie eine Partitionsaktion aus der Liste "Aktionstyp" aus. Die Aktionen sind unten aufgeführt:

HINWEIS: Die Bootumgebung und das Zielbetriebssystem müssen vor der Ausführung dieser Aktion festgelegt werden.

Partition erstellen: Hiermit können Sie eine Partition auf der angegebenen Festplatte erstellen.

- **Festplatte:** Geben Sie die Festplattenkennung ein. Unter Windows ist dies die Festplattennummer. Unter Linux ist es der Name der Festplatte.
- **Partitionstyp:** Wählen Sie den Partitionstyp aus. Unterstützt werden "Primäre", "Erweiterte" oder "Logische".
- **Größe:** Die Größe der zu erstellenden Partition in MB.
- **Offset:** Eine Zahl (im 8-Byte-Format), die angibt, wie weit in der Festplatte Sie die Partition erstellen möchten.
- **Start:** Die Startposition der Partition (Zylindernummer).
- **Ende:** Die Endposition der Partition (Zylindernummer).

Partition entfernen: Hiermit können Sie eine Partition auf der angegebenen Festplatte löschen.

- **Von der Festplatte entfernen:** Geben Sie die Festplattenkennung ein. Unter Windows ist dies die Festplattennummer. Unter Linux ist es der Name der Festplatte.
- **Partitionskennung:** Die zu löschende Partitionsnummer.

Alle Partitionen entfernen: Hiermit können Sie alle Partitionen von der Festplatte löschen.

- **Von der Festplatte entfernen:** Geben Sie die Festplattenkennung ein. Unter Windows ist dies die Festplattennummer. Unter Linux ist es der Name der Festplatte.

Partition formatieren: Erstellen Sie eine Dateisystemstruktur auf einer Partition.

- **Logischer Laufwerkbuchstabe:** Der Laufwerksbuchstabe der zu formatierenden Partition (unter Windows).
- **Partition:** Der Gerätename der zu formatierenden Partition (Linux).
- **Dateisystem:** Unter Windows sind dies FAT, FAT32 und NTFS. Unter Linux sind dies die Dateisysteme ext2, ext3, reiserfs und linux-swap.
- **Schnellformatierung:** Markieren Sie dieses Kontrollkästchen, um eine Schnellformatierung der Partition durchzuführen.

Partition bereitstellen: Stellt eine Partition bereit.

- **Festplatte:** Die bereitzustellende Festplattennummer (Windows).
- **Partition:** Der Gerätename der Partition (Linux).
- **Partitionskennung:** Die bereitzustellende Partitionsnummer (Windows).
- **Dateisystem:** Unter Linux sind dies die Dateisysteme ext2, ext3 und reiserfs.
- **Bereitzustellender Dateipfad:** Der Name der bereitzustellenden Partition. Der Bereitstellungspunkt muss vorhanden sein (Linux).
- **Zu erstellender logischer Laufwerkbuchstabe:** Der Laufwerksbuchstabe der Partition, die bereitgestellt werden soll (Windows).

Bereitstellung der Partition aufheben: Hiermit können Sie die Bereitstellung einer Partition aufheben.

- **Festplatte:** Die Festplattennummer, deren Bereitstellung aufgehoben werden soll.
- **Partitionskennung:** Unter Windows die Partitionsnummer, deren Bereitstellung aufgehoben werden soll. Unter Linux der Gerätename der Partition.
- **Zu löschender logischer Laufwerkbuchstabe:** Der Laufwerksbuchstabe der Partition, deren Bereitstellung aufgehoben werden soll (Windows).
- **Aufzuhebender Bereitstellungspunkt:** Der Name der Partition, deren Bereitstellung aufgehoben werden soll (Linux). Der Bereitstellungspunkt muss vorhanden sein.

Bootfähig machen: Hiermit machen Sie eine Partition bootfähig.

- **Festplatte:** Die Laufwerksnummer, die bootfähig gemacht werden soll. Unter Windows ist dies die Festplattennummer. Unter Linux ist dies der Name der Festplatte.
- **Partitionskennung:** Die Partitionsnummer, die bootfähig gemacht werden soll.
- **Bootfähig:** Aktivieren Sie das Kontrollkästchen, um die Partition bootfähig zu machen.
- **Windows 7 / Windows Server 2008 R2 mit einer separaten Systempartition:** Aktivieren Sie dieses Kontrollkästchen, um eine separate Betriebssystempartition zu erstellen.
- **Betriebssystem-Partitionskennung:** Die Partitionsnummer für die separate Betriebssystempartition.

Partition erweitern: Erweitert die letzte Partition auf dem Laufwerk. Es muss freier Speicherplatz verfügbar sein.

- **Festplatte:** Die bereitzustellende Festplattennummer.
- **Partitionskennung:** Unter Windows die bereitzustellende Partitionsnummer. Unter Linux der Gerätename der Partition.
- **Größe:** Die neue Größe der Partition in MB (Windows). Wenn Sie hier nichts eingeben, wird die Partition auf den gesamten Festplattenspeicher erweitert.
- **Start:** Die Startposition der Partition (Zylindernummer).
- **Ende:** Die Endposition der Partition (Zylindernummer).

System patchen (nur Abschnitt "Systemkonfiguration")

Die Aktion "System patchen" scannt das Zielgerät nach Anfälligkeiten und repariert diese. Diese Aktion kann nur nach einer Konfigurationsaktion ausgeführt werden, die den Agenten für Softwareupdates installiert.

- **Nur scannen:** Scannt den Computer auf Anfälligkeiten.
- **Anfälligkeit scannen und reparieren:** Scannt den Computer auf Anfälligkeiten und repariert (sofern möglich) die Anfälligkeit.
- **Gruppe scannen und reparieren:** Scannt den Computer auf Anfälligkeiten und repariert die in der Gruppe enthaltenen Anfälligkeiten.
- **Anfälligkeitskennung:** Eine gültige Anfälligkeitskennung von Patch Manager. Wenn die Kennung ungültig ist, schlägt die Aktion fehl.
- **Gruppenkennung:** Eine gültige Gruppenkennung von Patch Manager. Wenn die Kennung ungültig ist, schlägt die Aktion fehl. Sie können auf die Schaltfläche für die Liste der Gruppenkennungen klicken, um eine Anfälligkeitsgruppe auszuwählen, die Sie erstellt haben.

Die Core-Anfälligkeitsdefinitionen sollten vor dem Ausführen dieser Aktion aktualisiert werden. Alle zu reparierenden Patches müssen auf den Core heruntergeladen werden, bevor eine der beiden Reparaturoptionen in dieser Aktion ausgeführt werden kann.

Neu starten/herunterfahren (alle Abschnitte)

Starten Sie den Server neu oder fahren Sie ihn herunter. Unmittelbar im Anschluss an die Aktion "Betriebssystem-Installation" muss ein Neustart erfolgen. Nach dem Neustart startet der Versorgungsagent die Vorlage neu, um mit der Durchführung der Versorgungstasks fortzufahren. Verwenden Sie die Aktion "Neustart", um vom Abschnitt "Systemmigration" zu den "Betriebssystem"-Abschnitten oder von den "Betriebssystem"Abschnitten zum Abschnitt "Systemkonfiguration" zu gelangen. Es werden mehrere Neustarts unterstützt.

- **Neu starten:** Fahren Sie den Server herunter und starten Sie ihn neu.
- **Herunterfahren:** Fahren Sie den Server nach Abschluss des Versorgungstasks herunter und schalten Sie ihn nicht wieder ein. Sie müssen sicherstellen, dass diese Aktion die letzte Aktion in der Vorlage ist, sonst werden zusätzliche Aktionen nicht abgeschlossen.
- **Starten in Verwaltetes WinPE (Virtueller Start):** Den Clientcomputer in eine verwaltete WinPE-Umgebung starten. Aktionen werden wie vom Coreserver angewiesen ausgeführt. Diese Option ist für Situationen gedacht, in denen in einem Netzwerk kein PXE-Server für die Versorgung zur Verfügung steht.
- **Timeout für Bestätigungsmeldung:** Geben Sie die Anzahl der Sekunden an, für die eine Bestätigungsmeldung angezeigt wird, bevor das Zeitlimit erreicht ist.

Text ersetzen (Alle Abschnitte)

Hiermit ersetzen Sie Text in einer bestehenden Datei.

- **Quellenpfad- und Dateiname:** Der Pfad und Dateiname der Datei, in der Text ersetzt werden soll.
- **Folgendes suchen:** Der vorhandene Text, der zu ersetzen ist.
- **Ersetzen durch:** Der Text, der anstelle des vorhandenen Textes eingefügt werden soll.
- **Erstes Vorkommen ersetzen, Alle Vorkommen ersetzen:** Ersetzen Sie den neuen Text entweder nur beim ersten Auftreten oder bei jedem Auftreten.

Skriptgesteuerte Installation (nur Abschnitt "Betriebssystem-Installation")

Installieren Sie ein Betriebssystem mithilfe eines benutzerdefinierten Skripts. Es kann nur eine Aktion geben, die ein Betriebssystem installiert.

Windows

- **UNC-Pfad zur Installationsquelle:** Dies ist der Pfad zur ausführbaren Datei in der Installationsquelle. Dieser Pfad muss im Abschnitt "Vor der Installation des Betriebssystems" bereitgestellt worden sein (Aktion "Laufwerk zuordnen").
- **Domäne\Benutzername:** Geben Sie den Domänen- und Benutzernamen für die Anmeldung bei dem Gerät ein, auf dem sich die ausführbare Dateien befinden.
- **Variable als Kennwort verwenden:** Markieren Sie dieses Kontrollkästchen, um eine Variable für das Kennwort zu verwenden. Diese Variable wird in den **Vorlagenvariablen** unter dem Datentyp **Private Daten** definiert. Geben Sie den Variablennamen in Prozentzeichen eingeschlossen (%Variablenname%) in das Feld **Kennwort** ein. Weitere Informationen finden Sie unter "Definieren einer Vorlagenvariablen" auf Seite 464.
- **Kennwort:** Geben Sie das Kennwort für die Anmeldung bei dem Gerät ein. Bestätigen Sie das Kennwort im Feld **Kennwort bestätigen**.
- **Zusätzliche Parameter für Setup:** Parameter, die an die Installationsdatei übergeben werden, wenn sie ausgeführt wird. Bei Winnt32 füllt das Versorgungsmodul das unattend-Argument (/unattend) und die source-Argumente (/s) automatisch aus. Diese Argumente werden aus dem im Winnt32-Pfad zur Verfügung gestellten Pfad und aus dem ausgewählten Skript generiert.
- **Installationsskript:** Die bei der Installation des Betriebssystems verwendete unattend-Datei.
- **Neustart erzwingen:** Markieren Sie dieses Kontrollkästchen, wenn nach der Installation des Betriebssystems ein Neustart erforderlich sein soll.

Linux

- **Verzeichnispfad von initrd:** Der Speicherort der ursprünglichen RAMdisk-Datei. Der Standard ist /x86pc/undi/provlinux/initrd.img.
- **Kernelspeicherort:** Der Speicherort des Linux-Kernels.
- **Zusätzliche Parameter für Neustart:** Parameter, die an initrd übergeben werden, wenn diese Datei ausgeführt wird.
- **Installationsskript:** Die bei der Installation des Betriebssystems verwendete unattend-Datei.

Dienst deinstallieren (nur Abschnitt "Systemkonfiguration")

Hiermit wird ein Dienst auf dem Zielgerät deinstalliert

- **Dienstname:** Der Name des zu deinstallierenden Dienstes.

Datei entpacken (alle Abschnitte)

Entpacken Sie den Inhalt eines Pakets in ein vorher festgelegtes Verzeichnis. Diese Aktion kann die Originalstruktur wiederherstellen.

- **Quellpfad und Dateiname:** Geben Sie Pfad und Dateiname des Pakets ein, das entpackt werden soll.

- **Zielpfad:** Das Verzeichnis, in dem das Paket entpackt werden soll. Handelt es sich hierbei um ein Verzeichnis/einen Ordner, so werden doppelt vorhandene Dateinamen überschrieben.
- **Zielverzeichnis erstellen, falls noch nicht vorhanden:** Wenn das Ziel nicht vorhanden ist, markieren Sie dieses Kontrollkästchen, um es automatisch zu erstellen.

Registrierung aktualisieren (nur Abschnitt "Systemkonfiguration")

Diese Aktion fügt der Registrierung Schlüssel oder Werte hinzu, entfernt sie oder importiert eine Registrierdatei (.reg). Unsachgemäßes Bearbeiten der Registrierung kann Ihrem System Schaden zufügen und es möglicherweise unbrauchbar machen. Bevor Sie die Registrierung ändern, sollten Sie von allen wichtigen Daten auf Ihrem Computer eine Sicherungskopie anfertigen.

Wählen Sie einen Vorgang in der Liste **Registrierungsoperation** aus.

- **Schlüssel löschen:** Hiermit lässt sich der erwartete Ordner und Pfad eines Registrierungsschlüssels entfernen.
- **Wert löschen:** Hiermit lässt sich der erwartete Wert des Schlüssels entfernen.
- **Schlüssel erstellen:** Hiermit können Sie einen Ordner auf der linken Seite des Registrierungseditor erstellen.
- **Importdatei:** Hiermit können Sie eine Registrierungsdatei importieren.
- **Wert festlegen:** Hiermit können Sie einen Wert erstellen. Die eingegebenen Daten werden als ein von der Liste **Typ** bestimmter Wert interpretiert.
- **Schüssel:** Hiermit können Sie den zu erstellenden oder löschenden Schlüssel eingeben.
- **Wert:** Hiermit können Sie den zu erstellenden oder löschenden Wert eingeben.
- **Messwert:** Geben Sie hier die Daten zur Speicherung in einem Wert ein.
- **Typ:** Hiermit können Sie einen Datentyp auswählen. Es kann sich hierbei um einen Zeichenfolgewert, einen erweiterten Zeichenfolgewert, einen Binärwert, einen DWORD-Wert, einen Multi-String-Wert oder einen QWord-Wert handeln.
- **Inhalt der Importdatei:** Geben Sie eine Beschreibung für die Registrierungsdatei ein, die importiert werden soll.
- **Daten von Registrierungsdatei importieren:** Geben Sie den vollständigen Pfad zur Registrierungsdatei ein oder suchen Sie mit **Durchsuchen**. Klicken Sie anschließend auf **Datei importieren**.

Warten (alle Abschnitte)

Halten Sie die Vorlagenausführung für eine gewisse Zeit an oder bis die benötigte Datei erstellt wurde.

- **Uhrzeit**: Hält die Ausführung der Vorlage für eine bestimmte Zeit an.
- **Wartezeit in Sekunden:** Geben Sie die Anzahl der Sekunden ein, für die die Vorlage angehalten werden soll.
- **Datei:** Die Ausführung der Vorlage wird angehalten, bis eine Datei erstellt wurde.
- **Datei, auf die gewartet werden muss:** Die Aktion wird angehalten, bis der angegebene Pfad und die Datei existieren. Diese Funktion ist nützlich, wenn eine Aktion verlangt, dass eine Datei von einer Anwendung installiert wird. Wenn die Datei erstellt wurde, wird die nächste Aktion in der Vorlage ausgeführt.

- **Maximale Wartezeit in Sekunden:** Geben Sie die Anzahl der Sekunden an, für deren Dauer auf die Erstellung der Datei gewartet wird. Wenn die Zeit abgelaufen ist und die Datei nicht erstellt wurde, fährt die Vorlage mit der nächsten Aktion fort.

Vorlageneigenschaften

Die Ansicht **Vorlageneigenschaften** verwenden Sie, um die Vorlageninformationen anzuzeigen, die zum Zeitpunkt der Erstellung der Vorlage den aktuellen Informationen entsprachen.

So zeigen Sie Vorlageneigenschaften an

1. Klicken Sie auf **Extras > Verteilung > Betriebssystembereitstellung**.
2. Klicken Sie unter Versorgungsvorlagen auf **Öffentlich** oder **Eigene Vorlagen** oder eine Untergruppe.
3. Klicken Sie mit der rechten Maustaste auf eine Vorlage und klicken Sie dann auf **Eigenschaften**. Die folgenden Informationen werden angezeigt:

    - **Name der Vorlage:** Der Vorlagenname.
    - **Beschreibung:** Die Beschreibung der Vorlage.
    - **Name des Eigentümers:** Der Coreserver und Anmeldename der Person, die zur Ausführung der Vorlage berechtigt ist. Wenn sich die Vorlage in einem öffentlichen Ordner befindet, lautet der Name "Öffentlicher Benutzer".
    - **Bootumgebung:** Die Prebootumgebung, in die die Vorlage bootet (Windows PE).
    - **Zielbetriebssystem:** Das Zielbetriebssystem der Vorlage (z. B.: Windows, Windows Vista, Windows 2008 Server, Linux, SuSE Pro 9.3 oder Red Hat 4 Workstation).

Vorlagen im Ordner "Eigene Vorlagen" können von anderen Benutzern angezeigt, jedoch nur vom Ersteller der Vorlage oder von Benutzern mit Administratorrechten bearbeitet werden.

LANDesk SmartVue

Willkommen bei LANDesk SmartVue

Mit LANDesk® SmartVue können Sie wichtige Informationen zu IT-Prozessen anzeigen, die einen Einfluss auf die Benutzerproduktivität, die Systemleistung und die Endpunktsicherheit haben. SmartVue zeigt den Wert von IT innerhalb Ihres Unternehmens und ist das ideale Werkzeug für Leiter der PR-Abteilung (CIOs), Abteilungsleiter und IT-Direktoren, die für die Entscheidungsfindung und in geschäftlichen Gesprächen aktuelle Informationen benötigen.

SmartVue liefert Ihnen Daten zu den Erfolgen, Herausforderungen und Bedürfnissen Ihrer IT-Abteilung, die Sie gemeinsam nutzen können. Die Anwendung ermöglicht ferner die Verfolgung von Zielen, Service Level Agreements (SLAs) oder Key Performance Indicators (KPIs).

Mit SmartVue können Sie Grafiken und Diagramme auf Ihrem iPhone oder iPad anzeigen, die auf der Basis der auf Ihrem LANDesk Coreserver gespeicherten Management- und Sicherheitsdaten erstellt werden, wie etwa für:

- Verwaltete Geräte
- Betriebssysteme
- Patchprozesse
- Energieverwaltung
- Versorgung (Provisioning)
- Remotesteuerung
- Sicherheit
- Software
- Softwareverteilung
- Windows-Upgrades

Weitere wesentliche Funktionen:

- Gemeinsam nutzbare Informationen über PDF-Exporte
- Zeit- und Standortfilter für sämtliche Datensätze
- Direktes Drucken von Ihrem iPhone oder iPad aus dank Integration in iBooks
- Konnektivität mit anderen LANDesk Produkten wie z. B. Service Desk

Installieren von SmartVue

Das SmartVue-Installationsprogramm setzt einen LANDesk Management Suite 9.5 Coreserver voraus. Zwei Installationsarten stehen zur Verfügung:

- **Point-Core:** Ein Point-Core sammelt Daten von dem Coreserver, auf dem er installiert ist, und von anderen, von Ihnen spezifizierten Cores. Anschließend stellt der Point-Core diese Daten für die SmartVue Mobile-Anwendung bereit. Mehr als einen Point-Core sollten Sie in Ihrem Netzwerk nicht einrichten. Die Benutzeroberfläche für die SmartVue-Konfiguration befindet sich nur auf dem Point-Core.
- **Remote-Core:** Ein Remote-Core oder Slow-Link-Core sendet zur der von Ihnen festgelegten Zeit SmartVue-Daten an den Point-Core. Diese Installationsart sollten Sie für Cores in Erwägung ziehen, die über eine langsame Netzwerkverbindung mit dem Point-Core kommunizieren, oder aber für Cores, für die Beschränkungen hinsichtlich der Zugriffszeiten gelten.

Bei der Installation von SmartVue auf einem Point-Core werden die Widgets, die unterstützenden Webdienste und die Benutzeroberfläche für die Konfiguration installiert.

Bei der Installation von SmartVue auf einem Remote-Core werden nur zwei Dateien installiert: LDGatherData.exe und LANDesk.SmartVue.Shared.dll. Die ausführbaren Dateien können manuell in diesem Verzeichnis ausgeführt werden:

- C:\Programme (x86)\LANDesk\ManagementSuite\LDGatherData.exe

Dieses Programm sendet SmartVue-Abfragedaten an den Point-Core. Bei Remote-Cores müssen Sie die Ausführung dieser .EXE-Datei manuell zu dem von Ihnen gewünschten Zeitpunkt planen. Hierfür können Sie den Windows-Taskplaner oder den Local Scheduler von Management Suite verwenden.

So installieren Sie SmartVue auf einem Point-Coreserver

1. Falls die LDMS-Konsole auf dem Coreserver ausgeführt wird, auf dem die Installation erfolgen soll, beenden Sie diese.
2. Führen Sie die Datei Setup.exe von Ihrem SmartVue-Installationsabbild aus.
3. Klicken Sie auf der **Willkommen**sseite auf **Weiter**.
4. Klicken Sie auf der Seite **Lizenzvereinbarung** auf **Akzeptieren**.
5. Klicken Sie im Bildschirm **Voraussetzungen** auf **Weiter**.
6. Klicken Sie im Bildschirm **Was möchten Sie installieren?** auf **Point-Coreserver**. Wenn Sie SmartVue auf einem Remote-Coreserver installieren, klicken Sie auf **Remote-Coreserver** und klicken Sie dann auf **Weiter**.
7. Auf der Seite **Bereit zur Installation** klicken Sie auf **Installieren**.
8. Wenn das Setup abgeschlossen ist, klicken Sie auf **Fertig stellen**.

Im Anschluss an die Installation von SmartVue auf dem Point-Coreserver müssen Sie die SmartVue-Datensammlung planen und zusätzliche Datenquellen (sofern vorhanden) konfigurieren. Weitere Informationen finden Sie unter "Planen der SmartVue-Datensammlung" auf Seite 490 und "Konfigurieren von SmartVue-Datenquellen" auf Seite 491.

Planen der SmartVue-Datensammlung

Die SmartVue-Anwendung zeigt keine Echtzeitdaten an. Jedes Widget in der SmartVue-Anwendung basiert auf einer Reihe von Datenbankabfragen. Diese Abfragen müssen regelmäßig ausgeführt werden und die von der Anwendung angezeigten Daten entsprechen dann jeweils dem Stand der letzten Abfrage. Weitere Informationen finden Sie unter "Ändern von SmartVue-Widgets" auf Seite 494.

Wenn Sie SmartVue erstmals auf Ihrem Point-Core installieren, sollten Sie sofort einen Datensammlungszyklus starten, damit Daten zur Anzeige in der Anwendung zur Verfügung stehen.

So planen Sie einen sofortigen SmartVue-Datensammlungszyklus

1. Klicken Sie in der Managementkonsole auf **Konfigurieren > SmartVue-Konfiguration** und klicken Sie dann auf **Scheduler**.
2. Klicken Sie auf **Jetzt starten** und klicken Sie dann auf **OK**.
3. Überwachen Sie den Taskfortschritt im Extra "geplante Tasks". Klicken Sie auf **Extras > Verteilung > Geplante Tasks** und klicken Sie dann auf **Alle Tasks > SmartVue**.

Sobald einige SmartVue-Daten in der Datenbank vorliegen, sollten Sie einen Zeitplan für die regelmäßige Datensammlung konfigurieren. Die meisten Widgets tragen monatlich Daten zusammen. Ein Datensammlungslauf pro Tag funktioniert daher in der Regel ausgezeichnet.

So planen Sie einen regelmäßigen SmartVue-Datensammlungszyklus

1. Klicken Sie in der Managementkonsole auf **Konfigurieren > SmartVue-Konfiguration** und klicken Sie dann auf **Scheduler**.
2. Klicken Sie auf **Wiederholen**.

3. Wählen Sie **Stündlich**, **Täglich** oder **Wöchentlich** für den Zeitplan.
4. Konfigurieren Sie das gewählte Intervall.
5. Klicken Sie auf **OK**.

Konfigurieren von SmartVue-Datenquellen

Standardmäßig sammelt SmartVue Daten von dem Point-Core, auf dem es installiert wurde. Bei Bedarf können Sie weitere Datenquellen hinzufügen.

Das Dialogfeld **SmartVue-Konfiguration** bietet standardmäßig zwei Auswahlmöglichkeiten für die Datenquelle: **LANDesk Management Suite** und **LANDesk Service Desk**. Sollte die Datenbank, zu der Sie eine Verbindung herstellen wollen, einem dieser beiden Datenquellentypen entsprechen, sollten Sie unbedingt den passenden Typ auswählen.

Wenn Sie eine Verbindung zu einer benutzerdefinierten Datenquellen herstellen, können Sie Ihren eigenen Namen eingeben. Beachten Sie, dass bei dem von Ihnen hier eingegebenen Name für die **Datenquelle** zwischen Groß- und Kleinschreibung unterschieden wird und dieser Name ebenfalls in die XML-Datei für die Widgetkonfiguration eingegeben werden muss, die darauf Bezug nimmt. Das Attribut, das übereinstimmende Werte erfordert, ist das Attribut <DataDefinition datasource="">.

So konfigurieren Sie Datenquellen

1. Klicken Sie in der Managementkonsole auf **Konfigurieren > SmartVue-Konfiguration** und klicken Sie dann auf die Seite **Datenbank**.
2. Klicken Sie auf **Hinzufügen** oder wählen Sie eine vorhandene Datenquelle aus und klicken Sie dann auf **Bearbeiten**.
3. Geben Sie die Datenquelleninformationen und die Anmeldeinformationen für die Datenbank ein. Handelt es sich bei der Datenbank um eine Oracle-Datenbank, wählen Sie **Dies ist eine Oracle-Datenbank**. Klicken Sie auf **Hilfe**, um zusätzliche Informationen anzuzeigen.
4. Klicken Sie auf **OK**. Wenn der Point-Core auf der Basis der von Ihnen angegebenen Informationen keine Verbindung zu der von Ihnen konfigurierten Datenbank herstellen kann, wird eine Fehlermeldung angezeigt.

Konfigurieren von SmartVue-Standorten

Wenn Sie Geräte an mehreren Standorten verwalten, können Sie SmartVue so konfigurieren, dass Geräte nach Standort gruppiert werden. Verwenden Sie die Seite **Standort** (wählen Sie **Konfigurieren > SmartVue-Konfiguration** und klicken Sie dann auf die Seite **Standort**), um die Art und Weise zu definieren, wie SmartVue den Gerätestandort bestimmt. Drei Optionen stehen zur Auswahl:

- LDAP
- Gerätename
- LDMS - Öffentliche Abfragen

Sie können nur eine Methode für den Standort auswählen.

Konfigurieren von LDAP-Standorten

Wenn der Inventarscanner ein verwaltetes Gerät scannt, das zu einem Active Directory gehört, gibt der Scanner den Standortpfad des Geräts zurück. Sie können SmartVue mitteilen, welcher Teil des Pfads den standortbezogenen Text enthält, den Sie verwenden möchten.

Wählen Sie im Dialogfeld **SmartVue-Konfiguration** auf der Seite **Standort** die Option **LDAP**. Die Seite zeigt ein Beispiel für einen Standortpfad, der vom Inventarscanner gemeldet wurde. In dem Textfeld unterhalb des Beispielpfads sind die Elemente innerhalb des Pfads unter Verwendung des von Ihnen angegebenen Trennzeichens aufgeführt (/ ist das Standardtrennzeichen). Wählen Sie das Pfadelement, das den Standorttext enthält, den Sie in SmartVue verwenden wollen.

Konfigurieren von Standortangaben in Gerätenamen

Wenn Ihre Gerätenamen einen standardisierten Standortpräfix im Gerätenamen aufweisen (beispielsweise einen 3 Buchstaben umfassenden Städtenamen-Präfix), können Sie diesen hier eingeben. Sie müssen die Position des Startzeichens und die Länge eingeben. Wählen Sie die Zeichen in dem Beispieleintrag aus. Im Dialogfeld werden dann automatisch die Werte eingesetzt, die Ihrer Auswahl entsprechen. Beachten Sie, dass das erste Zeichen in einem Gerätenamen der Position 1 entspricht und nicht der Position 0.

Sie können nur eine Vorlage für Standortangaben in Gerätenamen konfigurieren.

Konfigurieren von Standorten für öffentliche LDMS-Abfragen

Wenn Abfrage vorliegen, die Computer nach Standort identifizieren, können Sie die Standortoption für öffentliche Abfragen verwenden. Die Ergebnisse einer jeden Abfrage entsprechen einem bestimmten Standort. Sie können mehrere Abfragen hinzufügen. Sobald Sie die gewünschten Abfragen ausgewählt haben, klicken Sie auf den **Standortnamen** der Abfrage und passen ihn an. Dieser **Standortname** wird dann in der Anzeige der Widget-Ergebnisse verwendet.

Verwenden der SmartVue iOS-App

Bevor Sie die SmartVue iOS-App verwenden können, müssen Sie folgende Schritte ausführen:

1. Installieren Sie SmartVue auf dem Coreserver, den Sie als Ihren Point-Core verwenden wollen. Weitere Informationen finden Sie unter "Installieren von SmartVue" auf Seite 489.
2. Planen Sie die Ausführung des SmartVue-Dienstprogramms für die Datensammlung (LDGatherData.exe) und führen Sie dieses Programm anschließend aus, damit Daten von Ihrem Point-Core für die SmartVue iOS-App zur Verfügung stehen.
3. Erteilen Sie den Benutzern der SmartVue-App die SmartVue-Berechtigung, damit sie sich von der Mobile-App aus beim Point-Core anmelden können (**Extras > Administration > Benutzerverwaltung**). LANDesk Administratoren verfügen standardmäßig über diese Berechtigung.
4. (Optional) Konfigurieren Sie zusätzliche Datenbankverbindungen zu weiteren Coreservern, LANDesk Service Desk-Servern oder benutzerdefinierten Datenquellen.
5. Installieren Sie die iOS-App auf Ihrem mobilen Gerät. Laden Sie die App "LD-SmartVue" von iTunes herunter: https://itunes.apple.com/us/app/ld-smartvue/id572070098.

Sobald die obengenannten Voraussetzungen erfüllt sind, können Sie sich bei Ihrem Point-Core anmelden.

So stellen Sie von der iOS-App aus eine Verbindung zum SmartVue Point-Core her

1. Starten Sie SmartVue auf Ihrem mobilen Gerät.
2. Geben Sie im Dialogfeld **Einstellungen** Ihren LANDesk **Benutzernamen** und Ihr **Kennwort** ein.
3. Die Core-URL lautet http://<Computername Ihres Point-Cores oder IP-Adresse>. Zum Beispiel: "http://eigenerLANDeskCore".

Sobald die Anwendung die Verbindung hergestellt hat, können Sie in den Daten blättern, die vom Dienstprogramm für die Datensammlung zusammengetragen wurden. Bei Fragen zur Verwendung der App sehen Sie in der Hilfe nach.

Die iOS-App stellt eine Verbindung zum Point-Core her, um die Widget-Daten abzurufen, wenn Sie eine Kategorie erstmals anzeigen und wenn Sie die Kategorien ändern. Die Navigation innerhalb einer Kategorie löst kein Update der Widget-Daten aus.

SmartVue-Architektur

Point-Cores verfügen über drei Webdienste. Diese Webdienste verwenden den vorhandenen STS-Token-Dienst auf dem Coreserver für die Authentifizierung bzw. Sicherheit.

- **SmartVueData:** Akzeptiert Daten, die von LDGatherData.exe gepostet wurden.
- **SmartVue:** Liefert Daten an die Mobile-Anwendung SmartVue.
- **Dashboard1:** Verwaltet die Widget-Anzeige in der Mobile-Anwendung SmartVue.

Setup erstellt die folgenden neuen Tabellen in der Datenbank:

- SmartVueData
- SmartVueLocationData
- SmartVueQueryLocations
- SmartVueWidgets
- SmartVueUserWidgets
- SmartVueConnections
- SmartVueSettings

LDGatherData.exe postet die Ergebnisse auf dem SmartVueData-Webdienst, der die Daten dann wiederum in die Tabellen SmartVueData und SmartVueLocationData stellt.

Bei langsamen Verknüpfungen wird LDGatherData.exe lokal installiert. Sie können die Ausführung dann für einen beliebigen Zeitpunkt planen. Bei der Ausführung von LDGatherData.exe werden die neuesten XML-Dateien vom Point-Core abgerufen und die Daten auf dem SmartVue-Webdienst des Point-Core gepostet.

Ändern von SmartVue-Widgets

Jede SmartVue-Widget-Kategorie ist in einer XML-Datei definiert, die vom SmartVue-Installationsprogramm auf dem Point-Core gespeichert wird. Sie können diese XML-Dateien ändern, indem Sie Widgets hinzufügen, ändern oder entfernen, die in der Mobile-Anwendung SmartVue angezeigt werden. Die XML-Dateien werden in folgendem Verzeichnis auf dem Point-Core gespeichert:

- C:\Programme (x86)\LANDesk\ManagementSuite\SmartVueDef.

HINWEIS: Beim Ausführen des SmartVue-Programms LDGatherData.exe wird ein .\SmartVue-Ordner erstellt, der ebenfalls XML-Dateien enthält. Diese Dateien dürfen keinesfalls bearbeitet werden. Wenn Sie eine .\SmartVueDef-XML-Datei ändern, wird die entsprechende Datei in .\SmartVue überschrieben, sobald LDGatherData.exe ausgeführt wird.

Stellen Sie sicher, dass Sie eine Sicherungskopie aller XML-Dateien erstellen, die Sie ändern möchten, bevor Sie irgendwelche Änderungen vornehmen.

Nachfolgend ist die grundlegende XML-Struktur gezeigt.

```
<?xml version="1.0" encoding="utf-8" ?>
<DataDefinition name="" id="" datasource="">
  <Definitions>
    <Definition name="" id="" controlType="" dataSet="">
      <Sql>
      </Sql>
      <TotalSQL>
      </TotalSQL>
      <LocationSQL>
      </LocationSQL>
      <Controls>
        <Control title="" columns="" />
      </Controls>
    </Definition>
  </Definitions>
</DataDefinition>
```

Jedes Widget enthält eine Widget-Definition und drei Sätze von Abfragen.

- **<SQL>:** Sammelt Daten für das Widget.
- **<Total SQL>:** Fragt die gesammelten SQL-Daten ab und gibt sie an das Widget zurück.
- **<Location SQL>:** Verbindet die Ergebnisse der <Total SQL>-Abfrage mit den Standortinformationen, die auf dem Point-Core konfiguriert wurden. Die Konfiguration von Standorten auf dem Point-Core erfolgt über **Konfigurieren > SmartVue-Konfiguration >Standort**. Sie können Standorte auf der Basis eines LDAP-Verzeichnisses, einer Präfixzeichenfolge für einen Computergerätenamen oder einer öffentlichen LDMS-Abfrage definieren.

Die folgenden Abschnitte enthalten weitere Details zur XML-Elementattributen.

<DataDefinition>

- **name:** Der Kategoriename. Dieser Name wird in der WHERE-Bedingung des <TotalSQL>-Abschnitts verwendet.
- **id:** Die eindeutige Kennung dieser Definition. Diese Kennung wird in der Browser-Abfragezeichenfolge verwendet. Leerzeichen und Zeichen wie "&" dürfen darin nicht enthalten sein.
- **datasource:** Der Datenbank-Datenquellentyp. Hier wird zwischen Groß- und Kleinschreibung unterschieden. Ferner ist eine genaue Übereinstimmung mit der von Ihnen im Dialogfeld **Datenbank hinzufügen** angegebenen **Datenquelle** erforderlich. (Wählen Sie **Konfigurieren > SmartVue-Konfiguration > Datenbank** und klicken Sie dann auf **Hinzufügen** oder **Bearbeiten**.)

<Definition>

- **name:** Der Widget-Titel. Dieser Name wird in der WHERE-Bedingung des <TotalSQL>-Abschnitts verwendet.
- **id:** Die eindeutige Kennung für dieses Widget. Leerzeichen dürfen darin nicht enthalten sein.
- **controlType:** Der für diese Daten zu verwendende Widget-Typ. Dieser muss einem der folgenden Typen entsprechen:
  - BarTemplate
  - BurnDownTemplate
  - ColumnTemplate
  - DonutTemplate
  - LineTemplate
  - PercentBallTemplate
  - PercentBarTemplate
  - PieTemplate
  - RadialTemplate
- **dataSet:** Das zurückgegebene Datenformat, entweder "row" (Zeile) oder "column" (Spalte). Beispiel: Wenn der Datensatz in einem Format zurückgegeben wird, bei dem Anzahl 1 in Spalte 1, Anzahl 2 in Spalte 2 und so weiter steht, liegt ein Datensatz im Spaltenformat ("column") vor. Wenn Ihre SQL-Anweisung mehrere Zeilen zurückgibt, muss das Datenformat "row" lauten.
- **seriesData:** Geben Sie "bymonth" (nach Monat) an, wenn dies für zeitbasierte Widget-Daten verwendet wird. Beispiele hierzu finden Sie in der Datei Remotecontrol.xml. Dies funktioniert sehr gut für Vorlagen auf der Basis von Balkendiagrammen.

<SQL> oder <SQLOracle>

Enthält die SQL- oder Oracle-Abfragen, die Daten für das Widget abrufen.

Wenn die SQL-Sprache bestimmte Oracle-Funktionen erfordert, können Sie die entsprechenden SQL-Anweisungen unter <SQLOracle> einschließen. Wenn es sich um generisches SQL handelt, ist dies nicht erforderlich. Dies gilt für alle Oracle-spezifischen Anweisungen.

<TotalSQL> oder <TotalSQLOracle>

Enthält die SQL- oder Oracle-Abfragen, die Daten für das Widget zurückgeben.

Die Reihenfolge und die Namen der Spalten spielen eine Rolle. Der Name der Spalte muss an erster Stelle stehen. Wenn Sie andere Bezeichnungen als "Data Count" oder "Count" wünschen, müssen Sie der erste Spalte den Alias "DataName" zuordnen (select a.columname DataName, …). Die Anzahl muss der zweiten Spalte der SELECT-Liste entsprechen und den Alias "DataCount" aufweisen. Wenn Zeilendaten vorliegen, muss dies eine Summe (SUM) sein. (select a.columnname DataName, SUM(a.DataCount) DataCount, …).

Wenn Ihre Daten anhand eines Datums (auf der X-Achse) angezeigt werden sollen, muss die letzte Spalte in der SELECT-Klausel dem Alias "ReportDate" entsprechen (select a.columnname DataName, SUM (a.DataCount) DataCount, a.ReportDate FROM …).

Die Bedingung a.CountType="" muss den Datendefinitionsnamen (<DataDefinition name="">) und den Definitionsnamen (<Definition name="">) enthalten, den Sie zuvor in der XML-Datei angegeben haben, und zwar ohne Leerzeichen zwischen den beiden Namen.

Beispiel: Für <DataDefinition name="Energieverwaltung"> und <Definition name="Geräte unter Energieverwaltung"> würde a.CountType= wie folgt lauten: "EnergieverwaltungGeräte unter Energieverwaltung".

Nicht-SQL-Elemente in den Abfragen des Abschnitts "TotalSQL"

#SVTABLE# ist ein Platzhalter, der verwendet wird, um zu bestimmen, ob Abfragen nach standortspezifischen Daten oder nicht standortspezifischen Daten suchen. Dieser Platzhalter wird dynamisch ersetzt.

Die Platzhalter #SVWHERE# und #SVTIME# werden verwendet, um zu bestimmen, ob die Abfrage auf dem Standort oder auf der Zeit basieren sollen, je nachdem, welche Auswahl der Benutzer in der Anwendung getroffen hat. Es gibt zwei Klassen von Widgets: zeitbasierte (zumeist als Balkendiagramme dargestellt) oder standortbasierte (zumeist als Tortendiagramme dargestellt). Mit standortbasierten Daten ist in der Regel keine Zeitspanne verknüpft. Zeitbasierte Widgets verwenden monatlich erfasste Daten.

<LocationSQL> oder <LocationSQLOracle>

Verbindet Daten mit Standorten.

Standorte legen Sie auf dem Point-Core fest, indem Sie auf **Konfigurieren > SmartVue-Konfiguration > Standort** klicken. Sie können Standorte auf der Basis eines LDAP-Verzeichnisses, einer Präfixzeichenfolge für einen Computergerätenamen oder einer öffentlichen LDMS-Abfrage definieren. Sie müssen sich für eine dieser Optionen entscheiden.

<Controls>, <Control title>

Definiert die Zeilen- oder Spaltendaten und -titel, die vom Widget angezeigt werden sollen. Dieser Abschnitt wird von SmartVue derzeit nicht verwendet.

Aktivieren von Widgets

Wenn Sie XML-Dateien im Ordner C:\Programme (x86)\LANDesk\ManagementSuite\SmartVueDef hinzufügen oder ändern, werden diese Änderungen in der Mobile-Anwendung SmartVue erst sichtbar, nachdem das folgende Programm für die Datensammlung ausgeführt wurde:

- C:\Programme (x86)\LANDesk\ManagementSuite\LDGatherData.exe

Wenn Sie einen Zeitplan für die Datensammlung für SmartVue definiert haben, erfolgt die Ausführung zum entsprechenden Zeitpunkt. Wenn die Ausführung sofort stattfinden soll, gehen Sie wie folgt vor.

So aktualisieren Sie SmartVue-Daten

1. Klicken Sie auf **Konfigurieren > SmartVue-Konfiguration > Scheduler**.
2. Klicken Sie auf **Jetzt starten**.
3. Klicken Sie auf **OK**.

Die Durchführung des LDGatherData.exe-Prozesses dauert ein paar Minuten.

Informationen zum Dialogfeld "SmartVue-Konfiguration"

Das Dialogfeld **SmartVue-Konfiguration** (**Konfigurieren > SmartVue-Konfiguration**) steht nur auf SmartVue-Point-Cores zur Verfügung. Dieses Dialogfeld verwenden Sie zum Konfigurieren von SmartVue-Datenbankverbindungen, Standortmethoden und Zeitplänen für die Datensammlung.

- "Informationen zur Seite "Datenbank"" auf Seite 497
- "Informationen zur Seite "Standort"" auf Seite 498
- "Informationen zur Seite "Scheduler"" auf Seite 498

Informationen zur Seite "Datenbank"

Die Seite **Datenbank** verwenden Sie, um Datenquellen für die Datenbank hinzuzufügen, aus denen SmartVue Daten sammeln soll. Weitere Informationen finden Sie unter "Konfigurieren von SmartVue-Datenquellen" auf Seite 491.

Informationen zum Dialogfeld "Datenbank hinzufügen"

- **Datenquelle:** Wenn Sie eine Verbindung zu einer Management Suite- oder Service Desk-Datenbank herstellen, treffen Sie die entsprechende Auswahl, anderenfalls geben Sie den Namen Ihrer benutzerdefinierten Datenquelle ein.
- **Anzeigename:** Ein aussagekräftiger Name für Ihre Datenquelle. Dieser Name wird in der primären Datenbankliste der SmartVue-Konfiguration angezeigt.
- **Server:** Der Name des Hostcomputers für die Datenbank, zu der Sie eine Verbindung hinzufügen.
- **Datenbank:** Der Datenbankname auf dem von Ihnen angegebenen Server.
- **Benutzername** und **Kennwort**: Datenbank-Anmeldeinformationen, die Zugriff auf die Datenbank gewähren.
- **Dies ist eine Oracle-Datenbank:** Diese Option wählen Sie, wenn es sich bei der Datenbank um eine Oracle-Datenbank handelt.

Wenn Sie auf **OK** klicken, verwendet SmartVue die von Ihnen angegebenen Informationen für die Herstellung der Verbindung zur Datenbank. Schlägt die Verbindung fehl, wird eine Fehlermeldung mit zusätzlichen Informationen angezeigt.

Informationen zur Seite "Standort"

Die Seite **Standort** verwenden Sie, um die Art und Weise zu konfigurieren, in der SmartVue den Gerätestandort bestimmt. Drei Optionen stehen zur Auswahl:

- LDAP
- Gerätename
- LDMS - Öffentliche Abfragen

Weitere Informationen finden Sie unter "Konfigurieren von SmartVue-Standorten" auf Seite 491.

Informationen zur Seite "Scheduler"

Über die Seite **Scheduler** steuern Sie, wann das Dienstprogramm für die SmartVue-Datensammlung (LDGatherData.exe) ausgeführt wird. Dieses Dienstprogramm sammelt Daten von dem Point-Core, auf dem es installiert ist und aus allen anderen Datenquellen, die von Ihnen konfiguriert wurden. Dieses Dienstprogramm wird nicht automatisch ausgeführt. Es gibt auch standardmäßig keinen Zeitplan für die Ausführung. Sie müssen einen Zeitplan erstellen oder das Dienstprogramm manuell ausführen.

Die Seite **Scheduler** bietet die folgenden Optionen:

- **Ungeplant lassen:** Dies ist die Standardeinstellung. Für die Ausführung von LDGatherData.exe gibt es keinen Zeitplan.
- **Jetzt starten:** LDGatherData.exe wird ausgeführt, sobald Sie auf **OK** klicken. Wenn Sie zuvor einen Zeitplan mit Wiederholungen konfiguriert hatten, wird dieser Zeitplan gelöscht. Wenn Sie im Anschluss an den Einsatz der Option **Jetzt starten** wieder zu einem Zeitplan mit Wiederholungen übergehen möchten, müssen Sie erneut **Wiederholen** wählen und den Zeitplan neu konfigurieren.
- **Wiederholen:** LDGatherData.exe wird gemäß dem von Ihnen festgelegten Zeitplan mit Wiederholungen ausgeführt. Als Intervalle für die Wiederholung stehen **Stündlich**, **Täglich** und **Wöchentlich** zur Wahl. Wenn Sie **Stündlich** wählen, wird der Zeitplan jede Stunde ausführt. Wenn Sie **Täglich** wählen, können Sie gewünschte Uhrzeit festlegen. Wenn Sie **Wöchentlich** wählen, können Sie den gewünschten Wochentag und die Uhrzeit festlegen.

Lokale Konten

Lokale Konten – Übersicht

Das Tool "Lokale Konten" ist ein Verwaltungswerkzeug, das dazu dient, die Benutzer und Gruppen auf lokalen Rechnern in Ihrem Netzwerk zu verwalten. Sie können von der Konsole aus Benutzer und Gruppen hinzufügen und löschen, Benutzer in Gruppen einfügen oder aus Gruppen löschen, Kennwörter einrichten und ändern, Benutzer- und Gruppeneinstellungen bearbeiten und Tasks zum Zurücksetzen von Kennwörtern für mehrere Geräte erstellen. Damit Verwaltung lokaler Konten möglich ist, muss der Standard LANDesk Agent installiert sein. Wenn ein Gerät ausgeschaltet oder nicht mit dem Netzwerk verbunden ist, können Sie "Lokale Konten" nicht zur Verwaltung des Geräts einsetzen.

HINWEIS: Beim Verwenden der lokalen Konten interagiert der Core praktisch in Echtzeit mit den anderen Geräten.

Verwalten lokaler Benutzergruppen

Sie können von der Konsole aus Gruppen auf einem lokalen Rechner hinzufügen, löschen und bearbeiten.

So fügen Sie eine Gruppe hinzu

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** mit der rechten Maustaste auf **Gruppen** und klicken Sie dann auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Neue Gruppe** einen Gruppennamen und eine Beschreibung ein.
5. (Optional) Fügen Sie Benutzer zur Gruppe hinzu, indem Sie auf **Hinzufügen** klicken.
6. Klicken Sie auf **Speichern**.

So löschen Sie eine Gruppe

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Gruppen**.
4. Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie auf **Ja**, um den Vorgang zu verifizieren.

So bearbeiten Sie eine Gruppe

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Gruppen**.

4. Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Nehmen Sie die gewünschten Änderungen an der Gruppe vor und klicken Sie dann auf **OK**.

Verwalten lokaler Benutzer

Sie können von der Konsole aus Benutzer auf einem lokalen Rechner hinzufügen, löschen und bearbeiten.

So fügen Sie einen Benutzer hinzu

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** mit der rechten Maustaste auf **Benutzer** und klicken Sie dann auf **Hinzufügen**.
4. Geben Sie in das Dialogfeld **Neuer Benutzer** einen Benutzernamen, einen vollständigen Namen und eine Beschreibung ein.
5. Geben Sie ein Kennwort ein, bestätigen Sie das Kennwort und geben Sie die Kennworteinstellungen an.
6. Klicken Sie auf **Speichern**.

So löschen Sie einen Benutzer

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie löschen möchten, und klicken Sie dann auf **Löschen**.
5. Klicken Sie auf **Ja**, um den Vorgang zu verifizieren.

So bearbeiten Sie einen Benutzer

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Nehmen Sie die gewünschten Änderungen an den Benutzereigenschaften vor und klicken Sie dann auf **OK**.

Zuweisen von Benutzern zu Gruppen

Es gibt zwei Methoden, mit denen Sie von der Konsole aus Benutzer auf einem lokalen Client zu Gruppen hinzufügen oder aus Gruppen entfernen können. Mit der ersten Methode können Sie mehrere Benutzer gleichzeitig zu einer Gruppe hinzufügen bzw. aus dieser entfernen. Mit der zweiten Methode können Sie einen ausgewählten Benutzer zu einer oder mehreren Gruppen hinzufügen bzw. aus diesen entfernen.

So fügen Sie Benutzer einer Gruppe hinzu

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Gruppen**.
4. Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
5. Klicken Sie im Dialogfeld **Gruppe bearbeiten** auf **Hinzufügen**.
6. Wählen Sie die Benutzer aus, die Sie der Gruppe hinzufügen möchten, und klicken Sie auf **Hinzufügen>>**.
7. Klicken Sie auf **OK**.
8. Klicken Sie im Dialogfeld **Gruppe bearbeiten** auf **OK**.

So fügen Sie einen Benutzer einer oder mehreren Gruppen hinzu

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie einer oder mehreren Gruppen hinzufügen möchten, und klicken Sie dann auf **Bearbeiten**.
5. Klicken Sie im Dialogfeld **Benutzer bearbeiten** auf die Registerkarte **Mitglied von**.
6. Klicken Sie auf **Hinzufügen**.
7. Wählen Sie die Gruppen aus, denen dieser Benutzer angehören soll, und klicken Sie auf **Hinzufügen>>**.
8. Klicken Sie auf **OK**.
9. Klicken Sie im Dialogfeld **Benutzer bearbeiten** auf **OK**.

So entfernen Sie Benutzer aus einer Gruppe

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Gruppen**.
4. Klicken Sie mit der rechten Maustaste auf die Gruppe, aus der Sie Benutzer entfernen möchten, und klicken Sie dann auf **Bearbeiten**.
5. Wählen Sie die Benutzer aus, die Sie entfernen möchten, und klicken Sie auf **Entfernen>>**.
6. Klicken Sie auf **OK**.

So entfernen Sie einen Benutzer aus einer oder mehreren Gruppen

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.

4. Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie aus einer oder mehreren Gruppen entfernen möchten, und klicken Sie dann auf **Bearbeiten**.
5. Klicken Sie im Dialogfeld **Benutzer bearbeiten** auf die Registerkarte **Mitglied von**.
6. Wählen Sie die Gruppen aus, aus denen dieser Benutzer entfernt werden soll, und klicken Sie dann auf **Entfernen>>**.
7. Klicken Sie auf **OK**.

Ändern des Kennworts eines lokalen Kontos

Sie können von der Konsole aus das Kennwort eines Benutzers ändern.

So ändern Sie das Kennwort eines Benutzers

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.
4. Klicken Sie mit der rechten Maustaste auf den Benutzer, für den Sie das Kennwort ändern möchten, und klicken Sie dann auf **Kennwort festlegen**.
5. Geben Sie ein neues Kennwort ein, bestätigen Sie das Kennwort und klicken Sie dann auf **OK**.
6. Klicken Sie auf **OK**, um zu überprüfen, ob das Kennwort erfolgreich geändert wurde.

Zurücksetzen des Kennworts eines lokalen Kontos

Sie können einen geplanten Task erstellen, um das Kennwort für einen bestimmten Benutzernamen zurückzusetzen. Nachdem die Planung des Tasks abgeschlossen ist, wird das Tool **Geplante Tasks** geöffnet; mit diesem Tool können Sie die Zielgeräte und Startzeit angeben. Beispiel: Sie können von einem lokalen Konto aus einen Task erstellen, mit dem das Kennwort für den Benutzernamen **Administrator** zurückgesetzt wird. Anschließend können Sie die Zielgeräte auswählen und festlegen, wann der Task ausgeführt wird. Sobald der Task ausgeführt wurde, müssen alle Administratoren, die sich bei den Zielgeräten authentifizieren, das neue Kennwort verwenden.

So setzen Sie das Kennwort zurück

1. Klicken Sie in der **Netzwerkansicht** der Konsole auf **Geräte > Alle Geräte**.
2. Klicken Sie mit der rechten Maustaste auf das Gerät, das Sie verwalten möchten, und wählen Sie **Lokale Benutzer und Gruppen verwalten** aus.
3. Klicken Sie im Dialogfeld **Lokale Benutzer und Gruppen** auf **Benutzer**.
4. Klicken Sie auf das Symbol **Planen**.
5. Geben Sie in das Dialogfeld **Task planen** den Benutzernamen ein, für den Sie das Kennwort zurücksetzen möchten. Sie können einen vorhandenen Benutzernamen aus der Liste auswählen oder einen anderen Namen eingeben.
6. Geben Sie ein neues Kennwort ein, bestätigen Sie das Kennwort und klicken Sie dann auf **Planen**.
7. Klicken Sie im Tool **Geplante Tasks** mit der rechten Maustaste auf den geplanten Task und klicken Sie dann auf **Eigenschaften**.
8. Wählen Sie im Dialogfeld **Geplante Tasks - Eigenschaften** die Zielgeräte aus und geben Sie die

Informationen für den Plan ein.

9. Klicken Sie auf **Speichern**.

Verwenden des Extras für lokale Konten auf dem Coreserver

Da Ihr Coreserver einen Knoten in Ihrem Netzwerk darstellt und über lokale Konten verfügt, können Sie das Tool "Lokale Konten" zum Durchführen administrativer Aufgaben auf dem Server sowie auf der eigentlichen Konsole verwenden. Sie können LANDesk Benutzer zur Konsole hinzufügen, indem Sie lokale Benutzer erstellen und zur Windows-Gruppe LANDesk Management Suite, LANDesk Script Writers oder LANDesk Administratoren hinzufügen. Auf diese Weise können Sie administrative Aufgaben von der Konsole aus wahrnehmen, ohne das systemeigene Verwaltungssystem für lokale Konten (z. B. Computerverwaltung unter Windows) verwenden zu müssen.

Je nach Präferenz können Sie zum Verwalten lokaler Konten dennoch das systemeigene Verwaltungssystem für lokale Konten verwenden. Sie können direkt auf die Geräte zugreifen, die Rechner von der Konsole aus remote steuern oder mit einem Tool eines anderen Anbieters auf die Geräte zugreifen und sie verwalten.

Weitere Informationen zum Verwenden der Konsole für die Verwaltung lokaler Konten finden Sie unter "Benutzerverwaltung" auf Seite 40.

Hilfe zur Verwaltung lokaler Konten

Informationen zum Dialogfeld "Neue Benutzer"

Mit diesem Dialogfeld erstellen Sie einen neuen Benutzer. Weitere Informationen finden Sie unter "Verwalten lokaler Benutzer" auf Seite 500.

- **Benutzername:** Gibt den Benutzernamen für den neuen Benutzer an.
- **Vollständiger Name:** Gibt den vollständigen Namen des Benutzers an.
- **Beschreibung:** Stellt eine Beschreibung des Benutzers zur Verfügung.
- **Kennwort:** Gibt ein Kennwort an, mit dem sich der Benutzer gegenüber der Konsole authentifizieren kann.
- **Kennwort bestätigen:** Bestätigt das Kennwort.
- **Benutzer muss Kennwort bei der nächsten Anmeldung ändern:** Veranlasst, dass der Benutzer sein Kennwort beim erstmaligen Anmelden an der Konsole ändern muss.
- **Benutzer kann Kennwort nicht ändern:** Lässt nicht zu, dass Benutzer das Kennwort ändern.
- **Kennwort läuft nie ab:** Veranlasst, dass das Kennwort nie abläuft, sodass der Benutzer das Kennwort nicht ändern muss.
- **Konto ist deaktiviert:** Deaktiviert das Konto.

Informationen zum Dialogfeld "Benutzer bearbeiten"

Mit diesem Dialogfeld können Sie die Benutzereigenschaften bearbeiten. Das Dialogfeld umfasst drei Konfigurationsregisterkarten: **Allgemein**, **Mitglied von** und **Profil**.

Weitere Informationen finden Sie unter "Verwalten lokaler Benutzer" auf Seite 500.

Registerkarte Allgemein"

Verwenden Sie diese Konfigurationsseite, um den Benutzernamen, den vollständigen Namen und eine Beschreibung des Benutzers einzugeben. Darüber hinaus können Sie einzelne Kontoeigenschaften ändern.

- **Benutzername:** Gibt den Benutzernamen des Benutzers an (sofern verfügbar).
- **Vollständiger Name:** Gibt den vollständigen Namen des Benutzers an.
- **Beschreibung:** Gibt die Beschreibung des Benutzers an.
- **Benutzer muss Kennwort bei der nächsten Anmeldung ändern:** Gibt an, ob Benutzer ihr Kennwort beim Anmelden an der Konsole ändern müssen.
- **Benutzer kann Kennwort nicht ändern:** Gibt an, ob Benutzer ihr Kennwort ändern können.
- **Kennwort läuft nie ab:** Gibt an, ob das Kennwort abläuft.
- **Konto ist deaktiviert:** Gibt an, ob das Konto deaktiviert ist.
- **Konto ist gesperrt:** Wenn ein Konto gesperrt ist, steht diese Option zur Verfügung. Konten werden in der Regal dann gesperrt, wenn ein Benutzer im Rahmen einer Sitzung mehr als drei Mal erfolglos versucht hat, sich bei seinem Konto anzumelden. Diese Option hebt die Sperrung des Kontos auf, damit sich der Benutzer gegenüber dem Betriebssystem authentifizieren kann.

Registerkarte "Mitglied von"

Verwenden Sie diese Konfigurationsseite, um den Benutzer Gruppen zuzuweisen.

- **Ausgewählte Gruppen:** Führt die Gruppen auf, denen der Benutzer angehört.
- **Hinzufügen:** Öffnet das Dialogfeld **Gruppen auswählen**. Hier können Sie die Gruppen hinzufügen, denen der Benutzer angehören soll.
- **Entfernen:** Entfernt den Benutzer als ein Mitglied der ausgewählten Gruppe und entfernt die Gruppen aus der Liste.

Profil

Verwenden Sie diese Konfigurationsseite, um die Kontoinformationen für den Benutzer anzugeben.

- **Benutzerprofil-Pfad:** Gibt den Netzwerkpfad für das Konto und Profil des Benutzers an.
- **Anmeldeskript:** Gibt die Anmeldeskripte an.
- **Lokaler Pfad:** Gibt einen lokalen Pfad als Stammverzeichnis an.
- **Verbinden:** Gibt ein Netzwerkverzeichnis als Stammverzeichnis an. Wählen Sie ein Laufwerk aus und fügen Sie dann den Netzwerkpfad ein.

Informationen zum Dialogfeld "Gruppeneigenschaften"

Verwenden Sie dieses Dialogfeld zum Konfigurieren der Gruppe. Weitere Informationen finden Sie unter "Verwalten lokaler Benutzergruppen" auf Seite 499.

- **Gruppenname:** Gibt den Namen der Gruppe an.
- **Beschreibung:** Stellt eine Beschreibung der Gruppe zur Verfügung.
- **Mitglieder:** Führt die Benutzer auf, die der Gruppe angehören.
- **Hinzufügen:** Öffnet das Dialogfeld **Benutzer auswählen**. Hier können Sie Benutzer zur Gruppe hinzufügen.
- **Entfernen:** Entfernt die ausgewählten Benutzer aus der Gruppe.

Verwalten von Macintosh-Geräten

Macintosh-Geräteverwaltung – Übersicht

LANDesk Management Suite bietet Systemverwaltungslösungen für Apple Macintosh-Computer und -Geräte und unterstützt Sie bei der Automatisierung vom Systemverwaltungstasks im gesamten Unternehmen. Die LANDesk Management Console bietet Ihnen folgende Möglichkeiten:

- Sammeln und Analysieren detaillierter Daten zum Hardware- und Softwareinventar eines jeden Geräts
- Verwendung dieser Daten für die Auswahl von Zielen für die Softwareverteilung und die Erstellung von Richtlinien für die automatisierte Konfigurationsverwaltung
- Verwaltung von Softwarelizenzen zur Einsparung von Kosten und Überwachung der Einhaltung von Lizenzverträgen (Compliance)
- Remotesteuerung von Geräten zur Behebung von Problemen oder zur Durchführung routinemäßiger Wartungsarbeiten
- Schutz Ihrer Geräte vor einer Vielzahl von weit verbreiteten Sicherheitsrisiken und Bedrohungen
- Verwaltung Ihres Inventars und Erstellung von aussagekräftige Berichten

Dieses Thema beschreibt, wie LANDesk Management Suite zum Verwalten von Macintosh-Computern verwendet wird. Es enthält spezifische Informationen zu Tasks, Extras, Features und Funktionalität im Zusammenhang mit Macintosh-Computern. Nähere Informationen zur Verwendung von Extras und Funktionen bei der Verwaltung Ihres Netzwerks finden Sie im Hilfethema zum jeweiligen Extra.

Unterstützte Betriebssystemversionen

Die Funktionalität von LANDesk Management Suite for Macintosh ist unter folgenden Versionen des Betriebssystems Mac OS X auf verwalteten Geräten nutzbar:

- 10.5 (Leopard)
- 10.6 (Snow Leopard)
- 10.7 (Lion)
- 10.8 (Mountain Lion)

Unterstützung für Legacyagenten

Mac OS X 10.2 (Jaguar), 10.3 (Panther), 10.4 (Tiger)

Der LANDesk Management Suite Agent Version 9.5 für Macintosh bietet keine Unterstützung für Jaguar, Panther oder Tiger. Sie können aber trotzdem Geräte verwalten, auf denen diese Betriebssysteme ausgeführt werden, sofern auf ihnen der LANDesk Management Suite Agent Version 8.8 für Macintosh installiert ist.

Informationen zum Download dieses Legacy-Agenten finden Sie im folgenden Dokument auf der Website der LANDesk Community: http://community.landesk.com/support/docs/DOC-21797.

HINWEIS: Aufgrund von Unterschieden in den Richtlinien zwischen der Version 8.8 und der Version 9.0 funktioniert die richtliniengestützte Verwaltung auf Jaguar- oder Panther-Clients, die den Agenten der Version 8.8 verwenden, nicht.

Mac OS 9

Inventar und Remotesteuerung werden auf Mac OS 9-Geräten unterstützt. Dieses Betriebssystem wird nicht mehr weiterentwickelt und wird daher nur noch eingeschränkt unterstützt.

Agentenkonfiguration für Macintosh-Geräte

LANDesk Management Suite verwendet zum Steuern und Verwalten von Geräten Agentenkonfigurationen. Macintosh-Agentenkonfigurationen werden per Push auf nicht verwaltete Macintosh-Geräte übertragen. Dabei wird auf denselben Prozess zurückgegriffen, der auch für das Pushen von Agenten auf Windows-Geräten verwendet wird.

Laden der Standard-Agentenkonfiguration für Macintosh-Geräte

Das Standard-Mac-Konfigurationspaket enthält den zum Steuern von Macintosh-Geräten erforderlichen Agenten. Um die Steuerung Ihrer Macintosh-Geräte zu übernehmen, müssen Sie Folgendes tun:

1. Besorgen Sie sich das erforderliche Paket (Agenten).
2. Stellen Sie die Agenten auf den Geräten bereit.

Nachdem Sie die Standardagenten installiert haben, sind Ihre Macintosh-Geräte verwaltbare Geräte. Jetzt können Sie benutzerdefinierte Konfigurationen erstellen, damit Sie diese Geräte noch gezielter steuern können. Benutzerdefinierte Agenten lassen sich einfach implementieren, sobald Ihre Geräte verwaltet sind.

HINWEIS: Alle Geräte müssen TCP/IP unterstützen.

Abrufen des Pakets (Agenten) für Macintosh-Geräte

Sie können das Standardpaket **Default_Mac_Configuration.mpkg.zip** im freigegebenen Ordner LDLogon/Mac auf Ihrem Coreserver finden. Der LDLogon/Mac-Order wird standardmäßig während der Installation von Management Suite erstellt. Da der LDLogon-Ordner eine Webfreigabe ist, ist er im Internet unter http://<CoreServerName>/LDLogon/Mac verfügbar.

Bereitstellen von Agenten auf Macintosh-Geräten, die Secure Shell (SSH) verwenden

Wenn Sie Agenten auf Macintosh-Geräte bereitstellen möchten, bei denen Secure Shell (SSH) aktiviert ist, müssen Sie die Anmeldeinformationen für die SSH-Anmeldung für nicht verwaltete Macintosh-Geräte angeben, indem Sie auf der Windows-Konsole **Konfigurieren > Dienste > Scheduler > Anmeldung ändern** wählen. Anschließend können Sie dieselbe pushbasierte Agentenbereitstellung verwenden, die Sie auch für Windows-Geräte verwenden würden.

Bereitstellen und Installieren von Agenten auf Macintosh-Geräten, die Secure Shell (SSH) nicht verwenden

Um Agenten auf Macintosh-Geräten zu platzieren, bei denen Secure Shell (SSH) nicht eingeschaltet ist, müssen Sie sich für eine der alternativen Bereitstellungsmethoden entscheiden, wie etwa folgende:

- Greifen Sie unter Verwendung eines Webbrowsers von LDLogon/Mac aus auf den Agenten zu und senden Sie die Konfigurationspakete per E-Mail an die Benutzer.

- Speichern Sie das Konfigurationspaket auf einer CD oder einem anderen mobilen Datenträger und suchen Sie damit jedes einzelne Macintosh-Gerät auf.

Nachdem Sie die Agenten auf den Zielgeräten bereitgestellt haben, müssen Sie sie auf den Geräten installieren. Am Ende eines jeden Installationsvorgangs wird ein vollständiger Hardware- und Softwarescan zur Synchronisierung der Geräte mit dem Coreserver ausgeführt. Um die Geräte verwalten zu können, müssen die LANDesk-Agenten auf Ihren Macintosh-Geräten installiert sein und die Inventarinformationen der Geräte an den Coreserver übermittelt werden. Nachdem Sie die Basisagenten installiert haben, werden künftige Agentenbereitstellungen und -aktualisierungen problemlos von den vorhandenen Agenten abgewickelt.

So installieren Sie den LANDesk Agenten auf einem Macintosh-Gerät

1. Suchen Sie auf dem Clientgerät die Datei **Default Mac Configuration.mpkg.zip** oder greifen Sie von der Webfreigabe (http://<CoreServerName>/LDLogon/Mac) aus auf dieses Paket zu.
2. Dekomprimieren Sie die Datei oder kopieren Sie die Dateien auf das Zielgerät.
3. Doppelklicken Sie auf **LDMSClient.mpkg**.
4. Wenn das Paket installiert worden ist, starten Sie den Computer neu.

Bereitstellen von Agentenkonfigurationen für Macintosh-Geräte

Verwenden Sie das Extra "Agentenkonfiguration", um benutzerdefinierte Konfigurationen für Ihre Macintosh-Geräte zu erstellen und zu aktualisieren (ersetzen). Sie können abgestimmt auf Ihre Anforderungen unterschiedliche Konfigurationen erstellen, beispielsweise mit geänderten Inventarscanner-Einstellungen, Remotesteuerungsberechtigungen oder von den Agenten zu verwendende Netzwerkprotokolle.

Um eine Konfiguration mit einem Pushvorgang auf Geräten bereitzustellen, müssen Sie eine Agentenkonfiguration erstellen oder aktualisieren und dann die Ausführung des Tasks planen.

Erstellen oder Aktualisieren der Agentenkonfiguration

Definieren Sie spezifische Konfigurationen für Ihre Geräte. Verwenden Sie keine Klammern in den Namen Ihrer Macintosh-Agentenkonfiguration. Klammern im Namen lassen den Bereitstellungstask scheitern.

So erstellen Sie eine Agentenkonfiguration für Macintosh-Geräte

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Wählen Sie eine Konfigurationsgruppe (**Eigene Konfigurationen** oder **Öffentliche Konfigurationen)** Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Agentenkonfiguration** > **Neue Macintosh Agentenkonfiguration**.
3. Geben Sie die erforderlichen Informationen in das Dialogfeld **Agentenkonfiguration** ein. Weitere Informationen finden Sie unter "Verwenden des Dialogfeldes "Agentenkonfiguration" (für Macintosh)" auf Seite 508 oder klicken Sie im Dialogfeld auf **Hilfe**.
4. Klicken Sie auf **Speichern**.

So aktualisieren Sie eine Agentenkonfiguration

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie mit der rechten Maustaste auf die zu aktualisierende Agentenkonfiguration und wählen Sie **Eigenschaften** aus.
3. Aktualisieren Sie die Agentenkonfiguration.
4. Klicken Sie auf **Speichern**.

Planen der Agentenkonfiguration

Sie können Agentenkonfigurationen mit einem Pushvorgang auf Geräten bereitstellen, auf denen der Standard LANDesk Agent installiert ist. Verwenden Sie das Extra **Geplante Tasks**, um Ihre neue oder aktualisierte Agentenkonfiguration bereitzustellen.

So planen Sie das Bereitstellen einer Agentenkonfiguration für Macintosh-Geräte

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie mit der rechten Maustaste auf die Agentenkonfiguration, deren Bereitstellung Sie planen möchten, und wählen Sie **Agentenbereitstellung planen** aus.
3. Ziehen Sie aus der Netzwerkansicht Geräte, Gruppen oder Abfragen auf den Task, um Zielgeräte für den Task festzulegen.
4. Wählen Sie den Task aus, klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** und geben Sie die Startzeit für den Task an.

Manuelles Ausführen von Agentenkonfigurationen für Macintosh-Geräte

Nachdem Sie Agentenkonfigurationen für Macintosh-Geräte erstellt oder aktualisiert haben, können Sie sie manuell ausführen. Beim Erstellen einer Agentenkonfiguration wird auf Ihrem Coreserver im LDLogon/Mac-Ordner die folgende Datei erstellt:

- **<Name der Agentenkonfiguration>.mpkg.zip**

Der LDLogon/Mac-Ordner ist eine Webfreigabe und sollte von jedem Browser aus erreichbar sein. Folgen Sie den Anweisungen für die Installation des Agenten (siehe "So installieren Sie den LANDesk Agenten auf einem Macintosh-Gerät" auf Seite 507), setzen Sie jedoch anstelle des Standarddateinamens den Dateiname Ihrer Agentenkonfiguration ein.

Deinstallieren der Macintosh-Agenten

Zur Deinstallation von Macintosh-Agenten führen Sie die Datei **uninstallmacagent.sh** im Verzeichnis \\<Core>\ldmain aus.

Verwenden des Dialogfeldes "Agentenkonfiguration" (für Macintosh)

Dieser Abschnitt beschreibt das Dialogfeld "Agentenkonfiguration" für Macintosh-Geräte Das Dialogfeld umfasst die folgenden Seiten:

- Start
- Verwaltung von Anwendungsrichtlinien (Application Policy Management)
- Inventar
- Remotesteuerung
- Standard LANDesk Agent
- Patch und Compliancescan
- Mandant

Informationen zur Startseite

- **Konfigurationsname**: Geben Sie einen eindeutigen Namen für die Agentenkonfiguration ein.
- **Standardkonfiguration**: Markieren Sie dieses Kontrollkästchen, wenn dies die Standard-Macintosh-Agentenkonfiguration sein soll.

- **Clientstatusmenü nicht ausführen**: Markieren Sie dieses Kontrollkästchen, wenn Sie nicht möchten, dass das Statusleistenmenü, mit dem Installationen und Scans ausgeführt werden können, für Endbenutzer sichtbar ist.

Informationen zur Seite "Application Policy Management"

Diese Seite verwenden Sie zur Konfiguration der Einstellungen für den richtlinienbasierten Verteilungsagenten.

- **TCP-Anschlussnummer:** Gibt an, welchen Anschluss der richtlinienbasierte Verteilungsagent für die Kommunikation mit dem Coreserver verwendet. Der Standardport ist 12176. Sie müssen sicherstellen, dass der Anschluss in allen Firewalls zwischen den Geräten und dem Coreserver offen ist. Wenn Sie diesen Anschluss ändern, müssen Sie ihn auch auf dem Coreserver ändern. Sie können den vom QIP-Serverdienst verwendeten Port ändern, indem Sie den folgenden Registrierungsschlüssel bearbeiten: HKLM\Software\Intel\LANDesk\LDWM\QIPSrvr
- **Ausführen wenn sich die IP-Adresse ändert:** Wenn diese Option markiert ist, löst jede Änderung der IP-Adresse einen Scan aus.
- **Einstellungen ändern:** Hier können Sie die Einstellungen ändern und einen benutzerdefinierten Zeitplan konfigurieren, der auf der Uhrzeit, dem Wochentag oder Monat aufbaut und davon abhängt, ob der Benutzer angemeldet ist oder nicht. Der Standardzeitplan umfasst einen täglichen Scan mit einer zufälligen Verzögerung von maximal einer Stunde.

Informationen zur Seite "Inventar"

Konfigurieren Sie mithilfe dieser Seite den Inventarscanner.

- **Scan an LDMS Coreserver senden:** Sendet die Scaninformationen an die Coreserver-Datenbank.
- **Scan in Verzeichnis speichern:** Das Verzeichnis, in dem die Scandaten gespeichert werden. Wenn Sie sowohl die Coreserver-Option als auch diese Option auswählen, werden die Scaninformationen an beide Speicherorte gesendet.
- **Scankomponenten auswählen:** Wählen Sie die Komponenten aus, die Sie scannen möchten. Wenn Sie nicht alle Komponenten auswählen, lässt sich die Geschwindigkeit u. U. leicht verbessern.
- **Softwarescan erzwingen:** Zwingt das Gerät, bei jedem Softwarescan einen Inventarscan auszuführen, unabhängig vom Zeitplan des Coreservers.
- **Ausführen wenn sich die IP-Adresse ändert:** Der an die IP-Adresse gekoppelte Trigger sendet nur einen Miniscan an den Coreserver. Dies beschleunigt den Inventarscan bei IP-Adressänderungen.
- **Einstellungen ändern:** Dient der Änderung von Einstellungen oder der Konfiguration eines benutzerdefinierten Zeitplans basierend auf der Uhrzeit, dem Wochentag oder Monat und ob der Benutzer angemeldet ist. Der Standardzeitplan legt fest, dass ein Scan jeden Tag mit einer willkürliche Verzögerung von bis zu einer Stunde ausgeführt wird.

Informationen zur Seite "Remotesteuerung"

Diese Seite verwenden Sie zum Konfigurieren des Remotesteuerungsagenten.

- **Lokale Vorlage:** Dies ist das einfachste Sicherheitsmodell, bei dem jede beliebige Remotesteuerungseinstellung verwendet wird, die auf dem Gerät definiert ist. Dieses Modell verlangt keine zusätzliche Authentifizierung oder Gruppenmitgliedschaft.
- **Integrierte Sicherheit:** Die sicherste Option. Bei der integrierten Sicherheit kommt folgender Kommunikationsfluss zum Einsatz:

1. Der Remote Control Viewer stellt eine Verbindung mit Remotesteuerungsagenten des verwalteten Geräts her. Daraufhin antwortet der Agent, dass die integrierte Sicherheitsauthentifizierung erforderlich ist.
2. Der Viewer fordert Remotesteuerungsrechte vom Coreserver an.
3. Der Coreserver ermittelt die angeforderten Remotesteuerungsrechte basierend auf dem Bereich des Viewers, der rollenbasierten Administrationsrechte und der Active Directory-Rechte. Anschließend erstellt der Coreserver ein sicher signiertes Dokument und sendet es zurück an den Viewer.
4. Der Viewer sendet dieses Dokument an den Remotesteuerungsagenten auf dem verwalteten Gerät. Dort wird die Prüfung des signierten Dokuments vorgenommen. Wenn alles seine Ordnung hat, lässt der Agent den Remotesteuerungsvorgang zu.

- **Berechtigung erforderlich:** Fordert den Benutzer auf, die Berechtigung zur Remotesteuerung zu erteilen, sobald ein Benutzer eine Remotesteuerungssitzung initiiert. Wenn der Benutzer nicht an der Tastatur sitzt oder die Berechtigung verweigert, wird die Remotesteuerungssitzung nicht gestartet.
- **Anwendungen und Dateien öffnen:** Ermöglicht es einem Remotebenutzer, Dateien auf diesem Gerät zu öffnen.
- **Elemente kopieren:** Mit dieser Option können Remotebenutzer Dateien auf dieses Gerät bzw. aus diesem Gerät kopieren.
- **Elemente löschen und umbenennen:** Ermöglicht es einem Remotebenutzer, Dateien, die auf diesem Gerät gespeichert sind, zu löschen oder umzubenennen.
- **Tastatur und Maus sperren:** Ermöglicht es einem Remotebenutzer, Ihre Tastatur und Maus während einer Remotesteuerungssitzung zu sperren. Diese Option verhindert, dass Sie Remotevorgänge behindern.
- **Bildschirm leeren:** Ermöglicht es einem Remotebenutzer, den Inhalt Ihres Bildschirm während einer Remotesteuerungssitzung auszublenden. Diese Option ist dann hilfreich, wenn sich auf Ihrem Gerät Dokumente mit vertraulichem Inhalt befinden, die ein Administrator ggf. per Remotezugriff öffnen muss. Mit dieser Option verhindern Sie, dass Personen, die an Ihrem Gerätemonitor vorbeigehen, diese Dokumente lesen können.
- **Neu starten und herunterfahren:** Ermöglicht es einem Remotebenutzer, Ihr Gerät neu zu starten oder herunterzufahren.
- **Steuern und beobachten:** Ermöglicht es einem Remotebenutzer, Ihre Aktionen auf dem betreffenden Gerät per Remotezugriff zu überwachen. Der Administrator kann nichts tun, außer Ihre Aktionen zu beobachten.
- **Alarmieren während Beobachtung:** Wenn eine Remotesteuerungssitzung aktiv ist, wird in der Menüleiste ein Hinweis eingeblendet.

Informationen zur Seite "Standard LANDesk Agent"

Auf dieser Seite konfigurieren Sie die Agentensicherheit und den Verwaltungsbereich. Weitere Informationen zur Agentensicherheit finden Sie unter "Agentensicherheit und vertrauenswürdige Zertifikate" auf Seite 114. Weitere Informationen zum Bereich finden Sie unter "Benutzerverwaltung" auf Seite 40.

- **Vertrauenswürdige Zertifikate:** Führt die Zertifikate auf dem Coreserver auf. Der Client muss ein Zertifikat besitzen, das mit dem Zertifikat auf dem Coreserver übereinstimmt, damit die Agentenkommunikation autorisiert werden kann. Diese Zertifikate werden verwendet, um die Agentenkommunikation zu authentifizieren. Sie können einen Domänennamen oder eine IP-Adresse eingeben, die der Client für die Kommunikation mit dem Coreserver verwenden soll. Der Remotesteuerungsagent für Macintosh verwendet kein Zertifikat.

- **Pfad:** Definiert das Inventarattribut "Computerstandort" des Geräts. Die Bereiche werden von der rollenbasierten Administration zum Steuern des Benutzerzugriffs auf Geräte verwendet und können auf diesem benutzerdefinierten Verzeichnispfad basieren. Der Pfad ist optional.

Info über die Seite "Patch- und Compliancescan"

Diese Seite verwenden Sie, um den Zeitplan für Patch- und Compliancescans zu konfigurieren.

- **Einstellungen ändern:** Dient der Änderung von Einstellungen oder der Konfiguration eines benutzerdefinierten Zeitplans basierend auf der Uhrzeit, dem Wochentag oder Monat und ob der Benutzer angemeldet ist. Der Standardzeitplan legt fest, dass ein Scan jeden Tag mit einer willkürliche Verzögerung von bis zu einer Stunde ausgeführt wird.
- **Alternativen Updateserver verwenden**: Geben Sie einen anderen Coreserver an, der für Patch und Compliance-Updates verwendet werden soll, wenn der primäre Coreserver nicht verfügbar ist.
- **Scan- und Reparatureinstellungen**: Wählen Sie die Einstellungen aus, die Sie für Patch- und Compliancescans verwenden möchten.
- **Konfigurieren**: Dient der Anzeige aller verfügbaren Scan- und Reparatureinstellungen. Bearbeiten Sie die vorhandenen Einstellungen oder erstellen Sie neue Einstellungen und wählen Sie die Einstellungen aus, die Sie für Patch- und Compliancescans verwenden möchten.

Informationen zur Seite "Mandant"

Diese Seite verwenden Sie, wenn Sie über das Management Suite Add-on für die Mandantenverwaltung verfügen. Sie können damit einem Mandanten innerhalb Ihres Unternehmens eine Agentenkonfiguration zuweisen.

- **Dieser Konfiguration einen Mandanten zuweisen**: Markieren Sie dieses Kontrollkästchen, wenn diese Macintosh-Agentenkonfiguration nur in Verbindung mit einem Mandanten in Ihrem Unternehmen verwendet wird.
- **Einen Mandanten auswählen**: Wählen Sie einen Mandanten aus der Liste der verfügbaren Mandanten aus, die in der LANDesk Management Console definiert wurden.

Herstellen einer Verbindung zum Coreserver über die LANDesk Cloud Services Appliance

Es stehen zwei Optionen zur Verfügung, mit denen verwaltete Macintosh-Geräte so konfiguriert werden können, dass sie eine Verbindung über die LANDesk Cloud Services Appliance (vormals LANDesk Management Gateway) herstellen:

- Sie "pushen" die Konfiguration auf mobile Geräte, während diese an das lokale Netzwerk angeschlossen sind. Dies ist ein einfacher Weg, mobile Geräte so zu konfigurieren, dass sie eine Verbindung über die LANDesk Cloud Services Appliance herstellen können, nachdem die Verbindung zum lokalen Netzwerk getrennt wurde. Diese Art der Konfiguration stellt LANDesk Management Suite Funktionen über die Appliance bereit, ohne dass es hierzu einer manuelle Konfiguration jedes einzelnen verwalteten Geräts bedarf.
- Sie konfigurieren jedes verwaltete Gerät manuell für die Verbindungsherstellung über die LANDesk Cloud Services Appliance. Diese Art der Konfiguration stellt LANDesk Management Suite Funktionen über die Appliance bereit. Eine manuelle Konfiguration kann nur von einem Benutzer mit Administratorrechten auf dem Clientgerät durchgeführt werden.

Pushen der Konfiguration auf mobile Geräte, während diese an das lokale Netzwerk angeschlossen sind

- Nachdem Sie den Core für die Verbindung über die LANDesk Cloud Services Appliance konfiguriert haben, erstellen Sie sämtliche Agenten für Macintosh-Geräte neu und übertragen diese mithilfe eines Pushs auf die Geräte. Nähere Informationen finden Sie unter Konfigurieren der LANDesk Cloud Services Appliance (Management Gateway).

So konfigurieren Sie ein verwaltetes Gerät manuell

1. Starten Sie auf dem verwalteten Gerät im Order **Dienstprogramme** die Anwendung LANDesk Cloud Services Appliance.
2. Geben Sie den **Domänennamen** der Appliance an.
3. Wählen Sie die am besten geeignete Methode für die Verbindung zum LANDesk Core.
4. Fordern Sie ein Zertifikat an, indem Sie den Benutzernamen und das Kennwort eines LANDesk Konsolenbenutzers eingeben und dann auf **Anforderung** klicken.
5. Klicken Sie auf **Testen**, um die Verbindung vom verwalteten Gerät zur LANDesk Cloud Services Appliance zu testen.
6. Falls der Test misslingt, überprüfen Sie die von Ihnen eingegebenen Informationen und korrigieren Sie etwaige Fehler; klicken Sie dann erneut auf **Testen**, um sicherzustellen, dass die Verbindung funktionsfähig ist.
7. Wenn das verwaltete Gerät über einen Proxy auf das Internet zugreift, geben Sie die benötigten Proxyeinstellungen an.

Ausführen eines Inventarscans auf Macintosh-Geräten

Der Inventarscanner ist ein Dienstprogramm, mit dem Macintosh-Geräte der Coredatenbank hinzugefügt und Daten zur Hardware und Software des Geräts erfasst werden. Wenn Sie ein Gerät konfigurieren, ist der Inventarscanner eine der LANDesk Agent-Komponenten, die auf dem Gerät installiert werden. Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Ein Gerät gilt als verwaltet, sobald es einen Inventarscan an die Coredatenbank sendet.

Die ausführbare Scannerdatei für Mac OS X heißt **ldiscan** (UNIX unterscheidet zwischen Groß- und Kleinschreibung). Inventarscandateien werden lokal auf dem Client gespeichert und sind mit dem Core kompatibel. Sie können die Datei per E-Mail an den Core-Administrator senden und dann mit Drag-und-Drop in das ldiscan-Verzeichnis verschieben. Sie müssen die Erweiterung der Datei in .scn ändern.

Macintosh-Geräte können für die Durchführung eines Scans beim Starten, beim Anmelden, beim Reaktivieren und bei einer Netzwerkänderung konfiguriert werden. Außerdem können Sie über die Agentenkonfiguration den Inventarscan so planen, dass er in regelmäßigen Intervallen ausgeführt wird.

Scans werden von Macintosh-Inventarscanner verschlüsselt. Der Inventarscanner verwendet darüber hinaus Deltascans, sodass nach dem ersten vollständigen Inventarscan nachfolgende Scans nur die geänderten Daten an den Coreserver weiterleiten. Auf diese Weise wird der Bandbreitenverbrauch verringert.

Der Macintosh-Inventarscanner sucht im Ordner "Benutzerdefinierte Daten" unter dem Installationsordner des Agenten nach XML-Dateien, die zusätzliche Informationen enthalten, die vom Inventarscanner an den Coreserver weitergeleitet werden sollen. Diese zusätzlichen Informationen werden in der Inventarstruktur unter dem Knoten "Benutzerdefinierte Daten" angezeigt.

Mit dem Inventarscanner können Sie eine Übersicht oder eine komplette Aufstellung aller Inventardaten anzeigen. Sie können die Inventardaten drucken und exportieren. Sie können mit dem Inventarscanner zudem Abfragen definieren, Server zu Gruppen zusammenfassen und benutzerdefinierte Berichte generieren.

Softwarescans

Bei einem Softwarescan wird das Softwareinventar auf verwalteten Geräten ermittelt. Diese Scans benötigen mehr Zeit für die Ausführung als Hardwarescans. Softwarescans können mehrere Minuten beanspruchen, je nachdem, wie viele Dateien sich auf dem verwalteten Gerät befinden. Sie können das Intervall für den Softwarescan auf der Registerkarte **Konfigurieren > Dienste konfigurieren > Inventar** konfigurieren.

Alle im Ordner "Applications" (Anwendungen) installierten Anwendungen werden dem Knoten **Software > Anwendungsfamilien** in der Inventarstruktur hinzugefügt.

Scannerbefehlszeilenparameter

Sie können Befehlszeilenparameter zu den Kontexteigenschaften des Inventarscanners (ldiscan) hinzufügen, um ihn zu steuern. Bei der Option wird zwischen Groß- und Kleinschreibung unterschieden.

HINWEIS: Einstellungen in den Scaneinstellungen der Agentenkonfiguration werden nicht durch Befehlszeilenoption überschrieben, es sei denn, die Option **--ignore** ist gesetzt. Wird also beispielsweise die Option **-F** für einen vollständigen Scan angegeben, so wird kein Softwarescan durchgeführt, wenn der Softwarescan in den Einstellungen deaktiviert wurde.

Option	Name	Beschreibung
-c	--core <Pfad>	Gibt an, an welchen Core der Scan gesendet wird. Beispiel: -c spencercore2.landesk.com
-D	--Delta	Erzwingt einen Deltascan.
-e	--everything	Erzwingt einen vollständigen Hardware- und Softwarescan.
-F	--force	Erzwingt einen Softwarescan, selbst wenn keine der Softwarescan-Optionen in der Agentenkonfiguration ausgewählt wurde. Beispiel: [MACHINES_MACX] REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldiscan –F
-h	--help	Zeigt eine Liste mit Befehlszeilenoptionen an.
-i	--ignore	Ignoriert Einstellungen für Benutzer- und Servereinstellungen.
-l	--LdAppl <Pfad>	Gibt den Pfad für den alternativen LdAppl.ini-Pfad an.
-L	--Limit	Beschränkt den Download von LdAppl3.ini.
-o	--output <Pfad>	Gibt an, an welches Verzeichnis Sie die Scandatei senden möchten. Beispiel: -o /Users/spencer

Option	Name	Beschreibung
-P	--Print	Zeigt die Scaneinstellungen an, ohne dass gescannt wird.
-R	--reset	Setzt die Scandatenbank zurück.
-s	--sync	Führt einen Synchronisierungsscan durch (und impliziert -R).
-T	--send <Datei>	Sendet <Datei> an den Core.
-T	--mini	Führt einen Miniscan durch.
-v	--version <n>	Gibt formatierte Versionsinformationen zurück (1, 2 oder 3).
-v	--Verbosity <n>	Legt den Ausführlichkeitsgrad (fürs Debugging) fest.

Bearbeiten der LdAppl3.Template-Datei

Die LdAppl3.Template-Datei enthält die Inventarparameter des Scanners. Diese Vorlagendatei erkennt zusammen mit der Datei LdAppl3 das Softwareinventar eines Geräts.

Sie können den Abschnitt [LANDesk Inventar] der Vorlagendatei bearbeiten, um die Parameter zu konfigurieren, die festlegen, wie der Scanner das Softwareinventar erkennt. Standardmäßig ist LdAppl3.Template im folgenden Verzeichnis auf dem Coreserver gespeichert:

- \Programme\LANDesk\ManagementSuite\LDLogon

Diese Tabelle unterstützt Sie beim Bearbeiten des Abschnitts [LANDesk Inventar] in einem Texteditor.

Option	Beschreibung
MacMode	Legt fest, wie der Scanner Geräte auf Macintosh-Software scannt. Standard ist "Alle". Es gibt folgende Einstellungen: • **Aufgelistete:** Zeichnet die Dateien auf, die in LdAppl3 aufgeführt sind. • **Nicht aufgelistete:** Zeichnet Namen und Datum aller Dateien auf, deren Erweiterungen in der Zeile "MacScanExtensions" aufgeführt, jedoch nicht in LdAppl3 definiert sind. Mit dieser Methode lässt sich nicht autorisierte Software auf dem Netzwerk finden. • **Alle:** Findet Dateien, die über Erweiterungen verfügen, die in der Zeile "MacScanExtensions" aufgelistet sind.

Sie müssen die Option **Für Clients verfügbar machen** aktivieren, damit die MacModes heruntergeladen werden können. MacScanExtensions ist standardmäßig eingeschaltet. Mit dieser Standardeinstellung können sehr große Dateien (11 MB+) entstehen. Daher kann es sinnvoll sein, die Einstellung zu ändern.

HINWEIS: Die Verzeichnisse /Library oder /System sind standardmäßig von einem "MacScanExtensions"-

Scan ausgenommen. Damit wird die Größe der Scandatei reduziert. Die Verzeichnisse können in den Abschnitt "Einschließen" des Mac-Ordners eingefügt werden.

Nach benutzerdefinierten Daten scannen

Informationen zum Scannen nach benutzerdefinierten Daten finden Sie unter "Scannen nach benutzerdefinierten Daten auf Macintosh-Geräten" auf Seite 183.

Remotesteuerung von Macintosh-Geräten

Sie können ein Macintosh-Gerät von der Konsole auf die gleiche Weise remote steuern wie ein Windows-Gerät. Bevor Sie Tasks über Remotesteuerung ausführen können, müssen Sie eine Verbindung zum Zielgerät herstellen. Es kann nur ein Viewer gleichzeitig mit dem Gerät kommunizieren. Sie können jedoch mehrere Viewer-Fenster öffnen und verschiedene Geräte gleichzeitig steuern.

Wenn Sie eine Verbindung zu einem Gerät herstellen, werden Verbindungsmeldungen und Status im Bereich **Verbindungsmeldungen** (**Ansicht > Verbindungsmeldungen**) angezeigt. Die integrierte Sicherheit von Management Suite prüft nach, ob der die Remotesteuerungssitzung initiierende Benutzer über die erforderlichen Rechte verfügt und der Computer dem Bereich des Benutzers angehört. Die Daten werden während der Übermittlung im Netzwerk verschlüsselt.

HINWEIS: Die integrierte Sicherheit von Management Suite ist standardmäßig eingeschaltet.

Nähere Informationen zur Verwendung der Remotesteuerung in Management Suite finden Sie unter "Remotesteuerung" auf Seite 257.

Herstellen einer Verbindung zu einem Macintosh-Gerät

Sie können eine Verbindung zu einem Macintosh-Gerät herstellen und es remote steuern. Sie können außerdem die Funktionen für Chat, Dateiübertragung oder Remoteausführung verwenden.

So stellen Sie eine Verbindung zu einem Gerät her

1. Klicken Sie in der **Netzwerkansicht** mit der rechten Maustaste auf das Gerät, das Sie per Remotesteuerung bedienen möchten, und klicken Sie dann auf **Remotesteuerung**, **Chat**, **Dateiübertragung** oder **Remoteausführung**.
2. Sobald das Viewer-Fenster angezeigt wird und die Verbindung mit dem Remotegerät hergestellt wurde, können Sie jedes beliebige Remotesteuerungstool verwenden, das im Menü **Extras** zur Verfügung gestellt wird, beispielsweise Chat, Dateiübertragung, Neustart, Inventar oder Remotesteuerung.
3. Zum Beenden einer Remotesteuerungssitzung klicken Sie auf **Datei > Verbindung beenden**.

HINWEIS: Clipboard-Freigabe und Zeichenfunktionen werden auf Macintosh-Geräten nicht unterstützt.

Macintosh-Tastaturemulation

Auf einer Macintosh-Tastatur gibt es einige Tasten, die auf PC-Tastaturen nicht zu finden sind. Bei der Remotesteuerung eines Macintosh-Geräts werden die folgenden Tasten auf der PC-Tastatur verwendet, um eine Macintosh-Tastatur zu simulieren:

- Die Alt-Tasten sind der Command-Taste zugeordnet.
- Die Windows-Tasten sind der Optionstaste zugeordnet.

Im Fenster "Remote Control Viewer" muss die Option für die Systemtastenweitergabe aktiviert sein, damit die Zuordnung der Alt- und Windows-Tasten zu den entsprechenden Macintosh-Tasten weitergeleitet wird.

Remotesteuerung über die Befehlszeile

Sie können einen Mac-Computer von der Befehlszeile eines Computers steuern, auf dem der Remotesteuerungscontainer installiert ist. Verwenden Sie folgenden Befehl:

```
irccntr.exe /a[Clientname] /s[Corename]
```

Timeout für Inaktivität

Das Inaktivitätstimeout gibt eine Zeitspanne (standardmäßig 10 Minuten) an, nach deren Ablauf die Sitzung getrennt wird, wenn der Client in dieser Zeit keine Maus- oder Tastenbewegungen registriert hat. Ähnlich wie ein Bildschirmschoner hindert diese Funktion andere Benutzer daran, einen unbeaufsichtigten Remotecomputer zu bedienen.

Bereitstellen von Softwarepaketen für Macintosh-Geräte

Mit der Softwareverteilung können Sie Software- und Dateipakete auf Macintosh-Geräten mit Mac OS X in Ihrem Netzwerk bereitstellen.

Sie können Pakete mit Einzeldateien an Mac OS X-Geräte verteilen. Jedes verteilte Paket besteht aus nur einer Datei; der Agent versucht, die Datei zu installieren, sobald das Gerät die Datei erhalten hat. Jede Datei kann gedownloadet werden. Installationspakete (.PKG) können auch Verzeichnisse enthalten, die jedoch komprimiert sein müssen. Wenn die heruntergeladene Datei die Erweiterung .DMG, .PKG, .MPKG, .SIT, .SITX, .ZIP, .TAR, .GZ, .SEA, .APP, .SH oder .HQX besitzt oder es sich um ein Automator/Workflow-Paket handelt, dekomprimiert LANDesk die Datei vor der Rückgabe.

HINWEIS: Vergewissern Sie sich, dass in Stuffit Expander die Option zum Suchen nach neuen Versionen deaktiviert ist. Andernfalls wird die Softwareverteilung unter Umständen durch ein Dialogfeld unterbrochen.

Die Softwareverteilung unterstützt darüber hinaus die Verteilung von Shell-Skripten als Auftrag. Damit erhalten Sie eine noch größere Kontrolle über die Mac-Betriebssystemumgebung und können beinahe alle Konfigurations- oder Informationserfassungstasks auf einem Mac OS X-Gerät ausführen.

Sie können verwaltete Mac OS X-Verteilungen im Fenster "Geplante Tasks" planen und Mac OS X-Geräte als Verteilungsziele in das Fenster "Geplante Tasks" ziehen.

HINWEIS: Sie müssen den Mac OS X-Agenten von LANDesk auf den Zielgeräten installieren, damit Sie Dateien an diese Geräte verteilen können.

Ein Verteilungspaket besteht aus den Paketdateien, die Sie senden möchten, und aus Informationen zur Verteilung, die die Paketkomponenten und deren Verhalten beschreiben. Sie müssen das Paket erstellen, damit es zugestellt und ausgeführt werden kann. Die folgenden Anweisungen erläutern, wie die Softwareverteilung durchzuführen ist. Voraussetzung für eine erfolgreiche Verteilung ist das Vorhandensein des Pakets auf einem Netzwerk- oder Webserver. Zudem muss der Softwareverteilungsagent auf den Zielgeräten installiert sein.

Verteilen eines Softwarepakets an Macintosh-Geräte

Die Verteilung eines Pakets an die Geräte umfasst im Wesentlichen drei Schritte:

1. Erstellen eines Verteilungspakets für die Software, die Sie bereitstellen möchten
2. Erstellen einer Verteilungsmethode
3. Planen eines Softwareverteilungstasks

So erstellen Sie ein Verteilungspaket

1. Erstellen Sie das Paket, das Sie verteilen möchten.
2. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
3. Klicken Sie unter **Eigene Pakete**, **Öffentliche Pakete** oder **Alle Pakete** in der Symbolleiste auf **Neu** und wählen Sie **Neues Macintosh-Paket**.
4. Geben Sie im Dialogfeld **Macintosh-Eigenschaften** die Paketinformationen ein und ändern Sie ggf. die Optionen. Weitere Informationen zu den einzelnen Seiten finden Sie in der **Hilfe**.
5. Klicken Sie auf **Speichern**, wenn Sie den Vorgang abgeschlossen haben. Ihr Paket wird unter dem Strukturelement für den von Ihnen gewählten Pakettyp angezeigt.

So erstellen Sie eine Verteilungsmethode

1. Klicken Sie auf **Extras > Verteilung > Verteilungsmethoden**.
2. Erweitern Sie die Gruppe **Verteilungsmethode**, klicken Sie mit der rechten Maustaste auf die Verteilungsmethode, die Sie verwenden möchten und klicken Sie dann auf **Neue Verteilungsmethode**.
3. Geben Sie im Dialogfeld **Verteilungsmethode** die gewünschten Verteilungsdaten ein und ändern Sie nach Bedarf die Optionen. Weitere Informationen zu den einzelnen Seiten finden Sie in der **Hilfe**.
4. Klicken Sie auf **Speichern**, wenn Sie den Vorgang abgeschlossen haben. Ihre Methode wird unter dem Strukturelement für die von Ihnen ausgewählte Verteilungsmethode angezeigt.

HINWEIS: Wenn ein Paket einen Neustart erfordert, wird es den Neustart des Zielgeräts veranlassen, unabhängig davon, welche Option Sie im Dialogfeld **Verteilungsmethode** auf der Seite **Neu starten** ausgewählt haben. Die Option **Nie neu starten** wird bei der Macintosh-Paketverteilung nicht unterstützt, da dies die Stabilität und Bootfähigkeit der Zielgeräte gefährden könnte, wenn ein Paket den Neustart nicht wie erwartet initiieren kann.

So planen Sie einen Softwareverteilungstask

1. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Softwareverteilung**.
3. Geben Sie auf der Seite **Übersicht** den Namen und Zeitplan des Tasks ein. Kontrollieren Sie die anderen Optionen und klicken Sie auf **Ändern**, wenn Sie Änderungen vornehmen möchten.
4. Wählen Sie auf der Seite **Verteilungspaket** das von Ihnen erstellte Paket aus.
5. Wählen Sie auf der Seite **Verteilungsmethode** die gewünschte Verteilungsmethode aus.
6. Auf der Seite **Zielgeräte** sind keine Geräte aufgeführt. Geräte werden zu Zielgeräten für die Verteilung, nachdem Sie diese aus der Netzwerkansicht auf den Task im Extra "Geplante Tasks" gezogen haben.
7. Die Seite **Benutzerdefinierte Nachricht** gilt nicht für Macintosh-Paketverteilungen.

8. Die Seite **Task planen** gibt **Ungeplant lassen** vor, es sei denn, es liegen Zielcomputer vor.
9. Klicken Sie auf **Speichern**, wenn Sie den Vorgang abgeschlossen haben. Der Task wird im Extra **Geplante Tasks** angezeigt.
10. Um das Paket zu verteilen, ziehen Sie Macintosh-Geräte aus der Netzwerkansicht auf den Task. Sie können einzelne Geräte, Gruppen oder Abfragen auf den Task ziehen.

Die Verteilung beginnt unmittelbar. Verfolgen Sie den Fortschritt des Tasks im Fenster "Geplante Tasks".

Macintosh-Softwareverteilungsbefehle

Die Befehle der Macintosh-Softwareverteilung sind downloadbar, im Gegensatz zu einem Shell-Befehl. Download-Befehle beginnen entweder mit "http://" oder "ftp://". Per Definition ist es ein Shell-Befehl, wenn es sich nicht um einen Downloadbefehl handelt. Das folgende Beispiel veranschaulicht das Format des Downloadbefehls:

```
REMEXEC0=http://...
```

Ein Downloadbefehl führt keine Dateien automatisch aus. Nachdem die Datei auf die Geräte geladen wurde, können Sie sie mit einem Shell-Befehl ausführen. Dateien werden in das Verzeichnis /Library/Application Support/LANDesk/sdcache/ gedownloadet. Dies sollten Sie bei Ihren Shell-Befehlen beachten.

HINWEIS: Wenn Sie Dateien auf einem Windows 2003-Server bereitstellen, müssen Sie MIME-Typen für die Macintosh-Erweiterungen erstellen (beispielsweise .SIT), da der 2003-Server Ihnen andernfalls keinen Zugriff auf die Dateien gewährt. Der MIME-Typ muss nicht gültig sind, nur existieren.

Konfigurieren von Richtlinien für Macintosh-Geräte

Sie können auch Richtlinien für Macintosh-Geräte erstellen. Das Erstellen einer Macintosh-Geräterichtlinie ähnelt dem Erstellen einer Richtlinie für Windows-basierte Geräte. Für Macintosh-Geräte sind außerdem dieselben vorgeschriebenen, empfohlenen und optionalen Richtlinientypen verfügbar. Macintosh-Anwendungspakete müssen als einzelne Datei vorliegen. Die richtlinienbasierte Verwaltung prüft im Abstand von vier Stunden auf Richtlinienaktualisierungen. Für optionale oder empfohlene Richtlinien muss der Client-Benutzer das Fenster mit den LANDesk-Voreinstellungen öffnen und für die richtlinienbasierte Verteilung auf **Jetzt prüfen** klicken. Beim Targeting von Richtlinien unterstützen Macintosh-Geräte die richtlinienbasierte Verwaltung nicht nach Benutzernamen, sondern nur nach Gerätenamen.

Die richtlinienbasierte Verwaltung behandelt Macintosh-Anwendungsrichtlinienpakete wie folgt:

1. Download von Dateien in /Library/Applications/LANDesk/sdcache (wie bei Softwareverteilungsdownloads).
2. Wenn die gedownloadeten Dateien komprimiert sind, dekomprimiert die richtlinienbasierte Verwaltung die Dateien im Speicherort.
3. Wenn es sich bei dem Download um ein Datenträgerabbild handelt, aktiviert die richtlinienbasierte Verwaltung das Abbild, sucht nach der ersten Apple Package Installer-Datei auf dem aktivierten Volume, führt sie im Hintergrund aus und deaktiviert sie dann.
4. Wenn das Download eine Apple Package Installer-Datei ist, wird diese von der richtlinienbasierten Verwaltung im Hintergrund ausgeführt.

Außerdem unterstützt die richtlinienbasierte Verwaltung .dmg-Dateien mit EULAs.

HINWEIS: Einige Pakettypen unterstützen die Softwareverteilung nur ungenügend. (Installer Vise- und Installer Maker-Installationen arbeiten in der Regel mit der richtlinienbasierten Verwaltung nur unzufriedenstellend zusammen. Sie erfordern fast immer Benutzereingaben und können abgebrochen werden.)

So fügen Sie eine Macintosh-Clientrichtlinie hinzu

1. Klicken Sie auf **Extras > Verteilung > Verteilungsmethoden**.
2. Konfigurieren Sie ein richtlinienunterstütztes Push oder eine Methode für die Richtlinienverteilung für das Paket, das Sie verteilen möchten.
3. Klicken Sie auf **Extras > Verteilung > Geplante Tasks**.
4. Klicken Sie in der Symbolleiste auf die Schaltfläche **Softwareverteilung**.
5. Konfigurieren Sie den Task. Klicken Sie auf **Hilfe** auf der jeweiligen Seite, wenn Sie mehr Hilfe benötigen.

So aktualisieren Sie lokale Clientrichtlinien

1. Klicken Sie in der LANDesk Agent-Anwendung auf dem Macintosh-Gerät auf das Symbol **Verteilung**.
2. Klicken Sie auf **Jetzt prüfen** für die richtlinienbasierte Verwaltung.

So zeigen Sie installierte Richtlinien an

- Klicken Sie auf dem Macintosh-Gerät im Fensterausschnitt "Management Suite-Einstellungen" auf die Registerkarte **APM**.

Anzeigen der Benutzeroberfläche auf dem Client

Sie haben die Wahl, die Benutzeroberfläche beim Verteilen eines Softwarepaketes auf Client ein- oder auszublenden. Wenn der LANDesk Administrator im Rahmen eines Pushvorgangs ein Paket verteilt, für das der Benutzer eine Lizenzvereinbarung auswählen muss, muss das Paket mithilfe einer benutzergesteuerten Verteilungsmethode installiert werden, da das Paket nicht installiert wird, wenn der Endanwender die Lizenzvereinbarung nicht akzeptiert. Sie können die Benutzeroberfläche sowohl für eine pushbasierte als auch richtlinienbasierte Verteilungsmethode anzeigen.

So zeigen Sie die Benutzeroberfläche während der Softwareverteilung auf dem Client an

1. Erstellen Sie eine neue Softwareverteilungsmethode oder wählen Sie eine vorhandene Methode zur Bearbeitung aus
2. Wählen Sie in der Strukturansicht **Feedback und Timing**.
3. Wählen Sie in der Liste **Benutzerschnittstelle für Paketfortschritt** den Eintrag **Fortschritt auf dem Bildschirm des Benutzers anzeigen**.
4. Wählen Sie **Vollständige Paketoberfläche anzeigen**.
5. Klicken Sie auf **Speichern**.

Ausführen von benutzerdefinierten Tasks mit verwalteten Skripten

LANDesk Management Suite verwendet Skripte zur Ausführung benutzerdefinierter Tasks auf Geräten. Skripte können im Fenster **Skripte verwalten** (**Extras > Verteilung > Skripte verwalten**) erstellt werden. Macintosh-Skripte verwenden Shell-Befehle zum Ausführen von Dateien. Shell-Befehle werden als Root ausgeführt. Die Skripte werden als Textdateien gespeichert und können nach ihrer Erstellung von Ihnen manuell bearbeitet werden. Das folgende Beispiel veranschaulicht einen Befehl:

```
REMEXEC0=/Library/Application\ Support/LANDesk/bin/ldscan
```

Benutzer können mit dem Shellbefehl "open" Dateien und Anwendungen starten oder mit "installer" .pkg-Dateien installieren. Die Downloaddatei kann auch ein in Perl, Ruby, Python usw. geschriebenes Shell-Skript sein.

Heruntergeladene Dateien werden unter /Library/Application Support/LANDesk/sdcache/ gespeichert; dies ist für die Ausführung von einigen Ihrer Shell-Befehle von Bedeutung.

Sie können verwaltete Mac OS X-Skripte im Fenster "Geplante Tasks" planen und Mac OS X-Geräte als Skriptziele in das Fenster "Geplante Tasks" ziehen.

Ausführen von geplanten Tasks auf Macintosh-Geräten

Das Extra "Geplante Tasks" aktiviert oder startet viele Tasks, die Sie in der Anwendung einrichten oder konfigurieren. Sie können die Tasks sofort ausführen und sie für die Ausführung zu einem späteren Zeitpunkt oder für die Ausführung in regelmäßigen Abständen konfigurieren.

Weitere Informationen finden Sie unter "Planen von Tasks" auf Seite 242.

HINWEIS: Damit Sie die Ausführung von Tasks für ein Gerät planen können, muss auf dem Gerät der Standard LANDesk Agent installiert und das Gerät in der Inventardatenbank registriert sein.

Das folgende Verfahren erfordert die Verwendung des Extras "Geplante Tasks":

- Bereitstellung der Agentenkonfiguration
- Softwareverteilung
- Verwaltete Skripte
- Bereitstellung des Betriebssystems
- Sicherheits- und Patchmanagement

Softwarelizenzüberwachung und zugehörige Berichte

Macintosh-Geräte, die Mac OS X ausführen, unterstützen die Softwarelizenzüberwachung. Bei jedem Inventarscan sendet der Macintosh-Agent für die Softwareüberwachung Informationen über die von den Geräten ausgeführten Anwendungen an den Coreserver. Das Extra "Softwarelizenzüberwachung" zeigt Macintosh-Anwendungen und Windows-Anwendungen.

Sie können nach Dateien anhand ihrer Erweiterungen suchen. Die LdAppl3.ini-Datei enthält die Liste der Erweiterungen, nach denen gescannt werden soll. Standardmäßig wird nach den Dateitypen .DMG und .PKG gesucht. Sie können zusätzliche Erweiterungen in die LdAppl3.ini-Datei einfügen, die sich standardmäßig im Ordner /Library /Applications /System /User befindet. Der Dateispeicherort kann ebenfalls geändert werden. Sie können die LdAppl3.ini-Datei auch zum Scannen nach Multimediadateien verwenden.

Die LANDesk Agent-Anwendung kann dazu verwendet werden, Anwendungen anzuzeigen, die gestartet wurden, und wie häufig diese verwendet wurden.

Erstellen von Berichten für Macintosh-Geräte

Mit dem Extra "Berichte" können Sie eine Vielzahl von Spezialberichten erstellen, die wichtige Informationen zu den verwalteten Macintosh-Geräten in Ihrem Netzwerk bereitstellen. Die Funktionsweise des Extras zur Berichterstellung ist für alle Betriebssysteme gleich. Weitere Informationen hierzu finden Sie unter "Berichte" auf Seite 209.

Patch und Compliance für Macintosh-Geräte

Patch und Compliance ist eine umfassende, integrierte Sicherheitslösung, mit der Sie Ihre verwalteten Macintosh-Geräte vor einem breiten Spektrum vorherrschender Sicherheitsrisiken schützen können. Sie können mit dem Extra Sicherheits- und Patchinhalte verwalten, Geräte scannen, Patches verwenden und Geräte reparieren.

Konfigurieren von Macintosh-Geräten für Sicherheitsscans und Reparaturen

Der Sicherheitsfunktionen sind Teil des Standard LANDesk Agenten für Macintosh-Geräte. Mit ihnen können Sie verwaltete Macintosh-Geräte auf Anfälligkeiten hin scannen und Reparaturen durch die Bereitstellung von Patches oder Softwareupdates durchführen.

Starten des Scanners für Macintosh-Geräte

Sie können den Scanner von der Konsole oder manuell vom Clientrechner aus starten.

So führen Sie einen Compliancescan von der LANDesk Management Console aus

1. Klicken Sie auf **Extras > Sicherheit und Compliance > Patch und Compliance**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Task erstellen** und wählen Sie **Compliancescan** aus.
3. Geben Sie einen Namen für den Task ein und wählen Sie **Geplanten Task erstellen** oder **Richtlinie erstellen**, je nachdem, wie der Scan ausgeführt werden soll.
4. Wählen Sie im Extra **Geplante Tasks** den Task aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften**.
5. Geben Sie die Scanoptionen an. Auf der Seite **Benutzerdefiniertes Skript** geben Sie die Details zum Compliancescan an.

Einzelheiten zum Erstellen eines Tasks für einen Compliancescan finden Sie unter "Erstellen von Tasks für Sicherheits- und Compliancescans" auf Seite 623.

HINWEIS: Wenn Sie Einstellungen für einen Compliancescan definieren, stehen einige Funktionen für

verwaltete Macintosh-Geräte nicht zur Verfügung. Wenn Sie auf die verschiedenen Elemente des Dialogfelds zeigen, wird durch eine Meldung angezeigt, wenn ein Element für Macintosh-Scans nicht zur Verfügung steht.

So starten Sie den Sicherheitsscanner auf einem Macintosh-Client

1. Öffnen Sie die **Systemeinstellungen** von MAC OS X auf dem Zielgerät und wählen Sie den Bereich **LANDesk Client** aus.
2. Klicken Sie auf der Registerkarte **Übersicht** im Abschnitt "Sicherheits- und Patch Management" auf **Jetzt prüfen**.

Blockieren von Anwendungen für Macintosh-Geräte

Das Extra "Management Suite Patch und Compliance" kann dazu verwendet werden, Anwendungen auf verwalteten Macintosh-Geräten zu blockieren. Diese Funktion arbeitet ähnlich wie die entsprechende Funktion für Windows-Geräte, mit dem Unterschied, dass für Macintosh-Geräte kein vordefinierter Blockinhalt verfügbar ist.

Sie können ausschließlich .app-Dateien auf verwalteten Macintosh-Geräten blockieren. Um bestimmte Anwendungen zu blockieren, müssen Sie für jede zu blockierende Anwendung eine benutzerdefinierte Definition erstellen. Stellen Sie sicher, dass Sie beim Erstellen der benutzerdefinierten Definition **Übernehmen für: Mac** auswählen.

Betriebssystembereitstellung (OSD) für Macintosh-Geräte

Sie können die Betriebssystembereitstellung (OSD, Operating System Deployment) mit dem LANDesk Agenten für Macintosh verwenden, indem Sie NetBoot/NetInstall als Teil Ihres Mac OS X Server einsetzen.

Detaillierte Informationen finden Sie in folgendem LANDesk Community-Dokument:
http://community.landesk.com/support/docs/DOC-5149

Zugriff auf ein Mac-Gerät mit dem Remote Control Viewer

Den "Remote Control Viewer" verwenden Sie, um aus der Ferne auf ein Gerät zuzugreifen. Sie können nur Windows und Mac Geräte remote steuern, auf denen der LANDesk-Agent installiert ist. Während einer Remotesteuerungssitzung haben Sie dieselben Rechte und Berechtigungen wie der auf dem Remotegerät angemeldete Benutzer. Sie können am Remotegerät die meisten Aktionen durchführen, die auch der Benutzer durchführen kann, der an diesem Gerät sitzt.

Sobald Sie die Steuerung eines Remotegeräts übernehmen, wird dessen Bildschirm im Viewer-Fenster angezeigt. Weil das Viewer-Fenster oft nicht so groß ist, wie der Bildschirm des Remotegeräts, müssen Sie entweder die Rollbalken zum Auf- und Ab- sowie Hin- und Herrollen oder die Funktion **Maßstab** zum Anpassen des Remotebildschirms verwenden, damit die Darstellungen auf dem Remotebildschirm in das Viewer-Fenster passen. Die Maßstabveränderung reduziert die Bildqualität, daher wird der Text unleserlich, wenn der Scaler die Bildschirmgröße stark verkleinern muss.

Sie können auch den Darstellungsbereich des Viewer-Fensters vergrößern, indem Sie im Menü **Sitzung** Elemente deaktivieren, z. B. die Chat- und Protokollfenster oder die Symbolleiste. Um alle Steuerelemente des Viewer-Fensters zu entfernen, wählen Sie im Menü **Ansicht** die Option **Vollbild**. Wenn die Auflösung des Remotebildschirms die Ihre übersteigt, wird sie Ihrem Bildschirm angepasst.

Wenn Sie die Anzeigerate beschleunigen oder die Viewer-Fenstereinstellungen ändern möchten, verwenden Sie die Option **Einstellungen** im Menü **LANDesk Remotesteuerung**, um den Dialog **Optionen** darzustellen.

Weitere Informationen finden Sie in den folgenden Abschnitten:

- Verbindungsherstellung zu Geräten
- Chat mit Remotegeräten
- Senden spezieller Tastenfolgen
- Verwenden der Remotesteuerung ohne die Anzeige des Remotebildschirms
- Anpassen der Remotesteuerung

Verbindungsherstellung zu Geräten

Bevor Sie Tasks über Remotesteuerung ausführen können, müssen Sie eine Verbindung zum Zielgerät herstellen. Es kann nur ein Viewer gleichzeitig mit dem Gerät kommunizieren. Sie können jedoch mehrere Viewer-Fenster öffnen und verschiedene Geräte gleichzeitig steuern. Wenn Sie eine Verbindung zu einem Gerät herstellen, sehen Sie die Verbindungsmeldungen und den Status im Fensterabschnitt "Protokoll", wenn dieser sichtbar ist. Andernfalls können Sie sie durch Klicken auf **Sitzung > Protokoll zeigen** darstellen.

Wenn Sie die eine neue Sitzung starten möchten, klicken Sie auf **Datei > Neu**. Um eine Sitzung zu beenden, klicken Sie auf **Datei > Schließen**. Wenn die Menüoptionen in **Sitzung** abgeblendet dargestellt sind, sind Sie nicht mit einem Gerät verbunden.

Chat mit Remotegeräten

Verwenden Sie den Remote Control Viewer, um mit einem Benutzer zu chatten, der an einem Remotegerät sitzt. Diese Funktion ist dann hilfreich, wenn Sie einem Remotebenutzer Anweisungen geben müssen, dessen Wählverbindung die einzige verfügbare Telefonleitung verwendet. Der Benutzer kann über das Chatfenster antworten, das auf seinem Bildschirm angezeigt wird. Chatten können Sie nur auf Geräten, auf denen der LANDesk-Agent für Mac installiert ist. Diese Funktion ist auch dann verfügbar, wenn Sie den Bildschirm des Remotegeräts nicht einsehen.

Sie können die Nachrichten aus einer Chatsitzung speichern. Der gesamte Text, der im grauen Bereich der Chatsitzung zu sehen ist, wird in einer Textdatei gespeichert.

So chatten Sie mit einem Benutzer an einem Remotegerät

1. Sobald Sie mit einem Remotegerät verbunden sind, klicken Sie auf **Sitzung > Chat anzeigen**.
2. Auf der rechten Seite des Anzeigefensters erscheint ein Chatrahmen. Der obere Abschnitt zeigt die gesendeten und empfangenen Nachrichten. Im unteren Abschnitt können Sie Ihre Nachricht eingeben. Drücken Sie auf **Eingabe**, um Ihre Nachricht zu senden.

Ihre Nachricht wird auf dem Bildschirm des Remotegeräts angezeigt. Der Benutzer kann antworten, indem er eine Nachricht eingibt und auf **Senden** klickt. Er kann auch auf **Schließen** klicken, um die Chatsitzung zu beenden.

So speichern Sie Nachrichten aus einer Chatsitzung

1. Klicken Sie im Chatbereich des Viewer-Fensters auf **Nachrichten speichern**.
2. Geben Sie einen Dateinamen im Dialogfeld **Speichern unter** ein und klicken Sie auf **Speichern**.

Senden spezieller Macintosh-Tastenfolgen

Auf einer Macintosh-Tastatur gibt es einige Tasten, die auf PC-Tastaturen nicht zu finden sind. Bei der Remotesteuerung eines Macintosh-Geräts werden die folgenden Tasten auf der PC-Tastatur verwendet, um eine Macintosh-Tastatur zu simulieren:

- Die Alt-Tasten sind der Command-Taste zugeordnet.
- Die Windows-Tasten sind der Optionstaste zugeordnet.

Im Fenster "Remote Control Viewer" muss die Option für die Systemtastenweitergabe aktiviert sein, damit die Zuordnung der Alt- und Windows-Tasten zu den entsprechenden Macintosh-Tasten weitergeleitet wird.

Verwenden der Remotesteuerung ohne die Anzeige des Remotebildschirms

Wenn Sie den Bildschirm des Remotegeräts nicht anzeigen, jedoch dennoch mit einem Benutzer am Remotegerät chatten möchten, können Sie die Beobachtung stoppen.

So stoppen Sie die Beobachtung eines Remotegeräts und erhalten dennoch eine Remotesteuerungsverbindung

1. Wenn die Verbindung zu einem Remotegerät hergestellt ist, klicken Sie auf **Sitzung > Nicht beobachten**. Sie können dennoch die Chatfunktion des Geräts verwenden.
2. Klicken Sie auf **Sitzung > Beobachten**, um die Remoteanzeige wiederherzustellen.

Anpassen der Remotesteuerung

Sie können die folgenden Remotesteuerungsoptionen anpassen:

- Ändern der Remotesteuerungseinstellungen
- Optimieren der Remotesteuerungsleistung
- Anpassen der Symbolleiste

Ändern der Remotesteuerungseinstellungen

Verwenden Sie zur Anpassung der Remotesteuerungseinstellungen die Registerkarte **Einstellungen** ändern (**LANDesk Remotesteuerung > Einstellungen**) im Dialogfeld **Optionen**.

- **Remotetastatur und -maus sperren:** Sperrt Tastatur und Maus des Remotegeräts, sodass nur der Benutzer, der mit dem Viewer arbeitet, das Remotegerät bedienen kann. Beachten Sie, dass bestimmte Tastenkombinationen in Windows, beispielsweise Strg-Alt-Entf oder Windows-Taste+L, nicht gesperrt sind.
- **Bildschirm des Remotecomputers ausblenden:** Leert den Bildschirm des Remotegeräts, sodass nur der Benutzer, der mit dem Viewer arbeitet, die Benutzeroberfläche auf dem Remotegerät einsehen kann.
- **Protokolleinträge in Remote.log schreiben:** Wenn Sie ein Protokoll der Remotesteuerungsaktionen in einer Protokolldatei auf einem Remotegerät speichern möchten, aktivieren Sie diese Option. Sie können aus drei Protokollierstufen wählen, wobei Stufe 1 am wenigsten umfassend und Stufe 3 am umfassendsten ist. Stufe 1 ist Standard.

Optimieren der Remotesteuerungsleistung

Verwenden Sie zur Anpassung der Remotesteuerungseinstellungen die Registerkarte **Leistung optimieren (LANDesk Remotesteuerung > Einstellungen)** im Dialogfeld **Optionen**.

Die Optimierung führt zu einer dynamischen Anpassung der folgenden Parameter: Farbreduzierung, Sichtbarkeit des Hintergrundbilds und Darstellung der Fenster auf dem Remotegerät (in Windows einstellbar über **Anzeige Eigenschaften > Darstellung > Effekte**), wie z. B. Übergangseffekte für Menüs und QuickInfo.

Zur Remotesteuerung von Daten wird immer ein hocheffizienter Kompressionsalgorithmus verwendet. Trotz Kompression müssen jedoch viele der Daten mit hoher Farbtiefe gesendet werden. Die Menge der zu sendenden Remotesteuerungsdaten kann durch Reduzierung der auf dem Remote Control Viewer angezeigten Farbtiefe erheblich verringert werden. Wenn der Viewer die Farbtiefe reduziert, muss er die volle Farbpalette vom remote gesteuerten Desktop einer reduzierten Farbpalette im Viewer zuordnen. Daher werden Farben im Remotesteuerungsfenster manchmal nicht genauso wie auf dem remote gesteuerten Desktop dargestellt. Falls dies ein Problem darstellt, sollte die Kompression auf eine höhere Qualität eingestellt werden.

Eine weitere Möglichkeit zur Leistungsoptimierung ist das **Unterdrücken des Hintergrundbilds auf dem remote gesteuerten Gerät**. In diesem Fall muss die Remotesteuerung keine Hintergrundbildaktualisierungen senden, wenn Teile des remote gesteuerten Desktops freigelegt werden. Hintergrundbilder benötigen oft eine hohe Bandbreite, z. B. wenn es sich um Fotos handelt. Diese lassen sich nicht gut komprimieren und brauchen bei langsameren Verbindungen lange für die Übertragung.

Anpassung der Symbolleiste für die Remotesteuerung

Sie können selbst einstellen, welche Schaltflächen auf der Remotesteuerungssymbolleiste erscheinen.

So passen Sie die Schaltflächen der Symbolleiste an

1. Klicken Sie auf **Sitzung > Symbolleiste anpassen**.
2. Ziehen Sie die gewünschten Schaltflächen von der Palette ins Viewer-Fenster.
3. Ziehen Sie die Schaltflächen, die Sie nicht wünschen, vom Viewer-Fenster auf die Palette.
4. Um das Standardlayout der Schaltflächen wiederherzustellen, ziehen Sie den Standardsatz unten auf der Palette ins Viewer-Fenster.

Sie können die Größe der Schaltflächen verändern, wenn Sie auf **Kleine Größe verwenden** klicken. Sie können auch die Option **Anzeigen** verwenden, um nur die Symbole oder nur den Text oder Symbole und Text anzuzeigen.

Einführung in LANDesk Security Suite

Willkommen bei LANDesk Security Suite

LANDesk®Security Suite stellt die Werkzeuge bereit, die Sie benötigen, um Geräte und kritische Daten in Ihrem Unternehmensnetzwerk über eine zentrale Konsole zu sichern und zu schützen.

LANDesk Security Suite unterstützt heterogene Netzwerkumgebungen mit Windows-, Macintosh- und Linux-Clients.

Die umfassende und mehrschichtige Sicherheitslösung Security Suite basiert auf den zentralen Funktionen von LANDesk Management Suite, mit denen Sie Netzwerkgeräte konfigurieren und verwalten können. Zusätzlich erweitert und optimiert wird diese Funktionalität durch die Bereitstellung von Sicherheitswerkzeugen wie Patch und Compliance, Antivirus, Endpunktsicherheit, HIPS, LANDesk Firewall, Gerätesteuerung, 802.1X NAC (Network Access Control), Agentenüberwachung und vieles mehr.

Eine umfassende und mehrschichtige Sicherheitslösung

LANDesk Security Suite ist eine optimal ausgestattete Sicherheitsverwaltungslösung, mit der Sie Ihre Netzwerkinfrastruktur und Ressourcen proaktiv *überwachen, bewerten, reparieren, verifizieren, schützen und stärken* können.

Das grundlegende Extra "Patch und Compliance" ermöglicht es Ihnen, die am weitesten verbreiteten Sicherheitsrisiken und -lücken, die eine fortlaufende Bedrohung für den Zustand und die Leistung Ihrer verwalteten Geräte darstellen, aufzuspüren und zu beseitigen. Zu diesen Risiken gehören: bekannte Betriebssystem- und Anwendungsanfälligkeiten, Spyware, Viren, Systemkonfigurationsfehler, unzulässige oder verbotene Anwendungen sowie andere potenzielle Sicherheitslücken.

Mit LANDesk Antivirus können Sie die neuesten Virendefinitionsdatei-Updates downloaden und Virenscans konfigurieren, die verwaltete Geräte auf Viren überprüfen. Außerdem können Sie Endanwendern Optionen für die Handhabung von Dateien, die infiziert und unter Quarantäne gestellt wurden, zur Verfügung stellen. Mit dem Extra "Gerätesteuerung" können Sie den Zugriff auf verwaltete Geräte über Netzwerkverbindungen und E/A-Geräte überwachen und beschränken.

Die nachstehende Tabelle verdeutlicht, wie sich die Security Suite Extras gegenseitig ergänzen und so ein stabiles, durchgängiges Schutzschild für Ihr System bilden.

Sicherheitsproblem / Task	LANDesk Security Suite Lösung
Wissen und Verifizierung	Konsolenansichten: • Sicherheitsinhaltslisten • Eigenschaften von Definitionen (und Erkennungsregeln) • Patch und Compliance-Scanergebnisse • Antivirusaktivität und Statusinformationen Alarme Berichte

Sicherheitsproblem / Task	LANDesk Security Suite Lösung
Patchmanagement	Patch und Compliance LANDesk-Aktualisierungen Treiberupdates Softwareupdates
Anfälligkeitsanalyse und Reparatur (bekannte, in der Branche veröffentlichte Definitionen, benutzerdefinierte Sicherheitsdefinitionen)	Patch und Compliance Downloads von Definitions- und Patchdateien Sicherheitsscans Compliancescans Patchbereitstellung und -installation Automatisches Korrigieren
Malware-Erkennung und -Reparatur	Antivirus • LANDesk Antivirus-Musterdatei-Updates und -Scans • Updates für Antivirus-Inhalte von Drittanbietern Spyware-Scans Riskware-Scans Echtzeitscans Anwendungsblocker
Gerätekonfiguration, Schutz vor Zero-Day-Angriffen und Sperre	Endpunktsicherheit • Standorterkennung (Netzwerkverbindungssteuerung) • Host Intrusion Prevention System (HIPS) • LANDesk Firewall • Gerätesteuerung • Listen der vertrauenswürdigen Dateien Sicherheitsbedrohungen (Anfälligkeiten der Systemkonfiguration) Windows-Firewallkonfiguration Agentenüberwachung
Network Access Control (Authentifizierung, Compliance mit Sicherheitsrichtlinie)	LANDesk 802.1X NAC-Unterstützung
Datenschutz	LANDesk Datenschutz mit Credant

Sicherheitsproblem / Task	LANDesk Security Suite Lösung
(richtlinienbasierte intelligente Verschlüsselung)	
Scan und Erkennung nicht verwalteter Geräte	Erkennung nicht verwalteter Geräte Erweiterte Geräteerkennung (ARP und WAP)

Sobald Sie LANDesk Security Suite installiert und Ihren Coreserver mit einer Security Suite-Lizenz aktiviert haben, können Sie sich in spezifischen Hilfethemen informieren, wie die Konsole gestartet und die verfügbaren Extras verwendet werden, einschließlich der weiter unten aufgeführten sicherheitsspezifischen Extras und Funktionen.

Navigieren Sie im LANDesk Help Center in den Hilfethemen zu LANDesk Management Suite und LANDesk Security Suite oder führen Sie eine Suche mit einem bestimmten Schlüsselwort oder Ausdruck durch, um die von Ihnen gewünschten Informationen zu finden.

WICHTIG: Security Suite enthält nicht alle Management Suite-Komponenten
Denken Sie daran, dass einige Management Suite-Komponenten nicht für die Security Suite-Implementierung gelten, z. B. die Betriebssystembereitstellung und Rollup-Cores.

Installieren und Aktivieren von LANDesk Security Suite

LANDesk Security Suite und LANDesk Management Suite installieren die erforderlichen Komponenten mit demselben Setupprogramm auf Ihrem Coreserver. Wie bei anderen LANDesk Softwareprodukten (z. B. Management Suite und Inventory Manager) werden die zutreffenden Security Suite Funktionen erst auf der Konsole zur Verfügung gestellt, wenn Sie den Coreserver mit Ihren LANDesk Kontoinformationen aktivieren.

Wenn Ihr Konto für LANDesk Security Suite lizenziert ist, werden die in den LANDesk Security Suite Hilfethemen beschriebenen Extras und Funktionen angezeigt, wenn Sie sich an der Konsole anmelden.

Ressourcen der LANDesk Benutzercommunity

Die Installation und Bereitstellung systemweiter Anwendungen wie der LANDesk Softwarelösung für das System- und Sicherheitsmanagement in einem heterogenen Netzwerk setzt ein wohl durchdachtes Vorgehen und eine umfassende Planung vor der Ausführung des Setupprogramms voraus.

Da die Anforderungen und Überlegungen bezüglich der Netzwerkinfrastruktur und der Skalierbarkeit der Datenbank bei Management Suite und Security Suite ähnlich sind und diese LANDesk Produkte dasselbe Setupprogramm verwenden, sollten Sie sich die Best Known Method (BKM)-Dokumente zur Installation und Bereitstellung (*Installation and Deployment*) ansehen, die Sie auf der Website des LANDesk Supports in der Benutzercommunity finden.

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter LANDesk Benutzercommunity – Startseite

Auf den Benutzercommunity-Seiten finden Sie mehrere nützliche Dokumente mit detaillierten Informationen zu Bereitstellungsstrategien und schrittweise Anleitungen für jede Phase der Bereitstellung, wie zum Beispiel:

- Erstellen einer Verwaltungsdomäne
- Vorbereiten der Datenbank
- Installation und Upgrade des LANDesk Coreservers
- Wissenswertes zu den verwendeten Ports
- Konfigurieren von Agenten für die Geräteverwaltung

LANDesk Security Suite Inhaltsabonnements

LANDesk Security Suite unterstützt Scan- und Reparaturvorgänge für zahlreiche unterschiedliche Sicherheitsrisiken, einschließlich bekannter Betriebssystem- und Anwendungsanfälligkeiten für unterstützte Geräteplattformen, Spyware, Viren, Systemkonfigurationsbedrohungen, nicht autorisierte Anwendungen usw. Jedes Sicherheitsrisiko, ganz gleich welchen Typs, wird anhand von Definitionsdateien identifiziert. Eine Definitionsdatei besteht normalerweise aus einer ID (Kennung), spezifischen Attributen, Erkennungsregeldetails und Informationen zur Patchdatei (sofern zutreffend).

LANDesk unterhält eine Datenbank mit validierten Sicherheitsdefinitionsdateien (auch Security Suite-Inhalte oder Sicherheits- und Patchinhalte genannt), die fortlaufend aktualisiert und verifiziert werden und über das Internet zum Download bereitstehen. Um Sicherheits- und Patchinhalt herunterladen zu können, müssen Sie im Besitz eines Security Suite-Inhaltsabonnements sein.

Informationen zu den Security Suite-Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.

LANDesk Startseite

Download von Sicherheitsupdates von LANDesk

Im Hilfeabschnitt "Patch und Compliance" erfahren Sie, wie Sie Sicherheits- und Patchinhalte, für die Sie ein Abonnement besitzen, herunterladen können. Weitere Informationen finden Sie unter "Download von Updates für Sicherheitsinhalte" auf Seite 600.

Verwandte Themen

"Security Suite Extras und Funktionen" auf Seite 529

Security Suite Extras und Funktionen

Das LANDesk Security Suite zugrunde liegende Extra heißt "Patch und Compliance". Nähere Informationen zu Sicherheitsinhalten und unterstützten Geräteplattformen und wie Sie das Extra "Patch und Compliance" für Sicherheits- und Compliancescans und Reparaturen einsetzen sowie Scanergebnisse anzeigen, Sicherheitsberichte generieren und fortwährende Systemsicherheit konfigurieren können, finden Sie unter "Patch und Compliance" auf Seite 578.

Dieses Hilfethema bietet eine kurze Übersicht über die folgenden von LANDesk Security Suite bereitgestellten Extras zur Sicherheitsverwaltung und Links zum Übersichtsthema des jeweiligen Extras:

- "Patch und Compliance" auf Seite 530
- "Konformität mit dem CVE-Benennungsstandard" auf Seite 530
- "Compliance mit Federal Desktop Core Configuration (FDCC)-Standards" auf Seite 531
- "Sicherheitsaktivität" auf Seite 531
- "Agenteneinstellungen" auf Seite 531

- "Endpunktsicherheit" auf Seite 531
  - "Host Intrusion Prevention System (HIPS) – Übersicht" auf Seite 719
  - "Konfigurieren der LANDesk Firewalleinstellungen" auf Seite 734
  - "Gerätesteuerung – Übersicht" auf Seite 740
  - "Informationen zur Endpunktsicherheit: Seite "Standortrichtlinien"" auf Seite 718
- "LANDesk Antivirus" auf Seite 532
- "LANDesk 802.1X NAC" auf Seite 533
- "LANDesk Datenschutz mit Credant" auf Seite 533
- "Häufig verwendete LANDesk Extras, die in Security Suite enthalten sind" auf Seite 533
- "Sonstige in Security Suite enthaltene LANDesk Management Suite-Funktionen" auf Seite 535
- "Zusätzliche Informationsquellen" auf Seite 536

Patch und Compliance

Patch und Compliance verwenden Sie, um (nebst anderen Sicherheitsinhaltstypdefinitionen) die neuesten bekannten Anfälligkeitsdefinitionen und ihre zugehörigen Patches herunterzuladen. Scannen Sie verwaltete Geräte sowie Coreserver und Konsolen auf vorhandene LANDesk Softwareupdates. Konfigurieren und starten Sie angepasste Sicherheitsanalyse-Scans für bekannte plattformspezifische Anfälligkeiten, Spyware, Sicherheitsbedrohungen für die Systemkonfiguration, Antivirusscanner und verweigerte oder unzulässige Anwendungen.

Das Extra "Patch und Compliance" unterstützt Sie ferner bei folgenden Aufgaben:

- Erstellen von eigenen benutzerdefinierten Sicherheitsdefinitionen, mit denen Sie Geräte auf potenziell gefährliche Bedingungen durchsuchen können
- Analysieren, Priorisieren, Laden, Verteilen und Installieren von Patches
- Erstellen und Starten von geplanten Tasks und Richtlinien, die erkannte Sicherheitsrisiken reparieren
- Festlegen, ob der Sicherheitsscanner während der Ausführung von Scan- und Reparaturvorgängen auf den Geräten von Endbenutzern angezeigt wird, Konfigurieren von Neustartoptionen und der Ebene der Interaktion mit den Benutzern
- Anzeigen von umfassenden Sicherheits- und Patchinformationen für gescannte Geräte
- Aktivieren der Sicherheitsalarmierung
- Erstellen von Sicherheitsberichten

Weitere Informationen finden Sie unter "Patch und Compliance" auf Seite 578.

HINWEIS: Patch und Compliance scannt eine LANDesk Management Suite-Implementierung
Das Extra "Patch und Compliance" ist standardmäßig in einer LANDesk Management Suite-Installation (Coreserver-Aktivierung) enthalten. Anfänglich können Sie jedoch nur nach LANDesk Softwareupdates und ihren eigenen benutzerdefinierten Sicherheitsdefinitionen scannen. Um zusätzliche Sicherheitstypen durchsuchen und reparieren zu können, benötigen Sie das entsprechende Security Suite-Inhaltsabonnement.

Konformität mit dem CVE-Benennungsstandard

LANDesk Security Suite-Produkte unterstützen den Benennungsstandard nach CVE (Common Vulnerabilities and Exposures). Mit Patch und Compliance können Sie anhand des CVE-Namens nach Anfälligkeiten suchen und CVE-Informationen für heruntergeladene Anfälligkeitsdefinitionen anzeigen.

Weitere Informationen zur CVE-Benennungskonvention, zur LANDesk Kompatibilität mit dem CVE-Standard und dazu, wie Sie mithilfe der CVE-Kennung individuelle Anfälligkeiten in Patch und Compliance finden können, finden Sie unter "Suchen nach Anfälligkeiten anhand des CVE-Namens" auf Seite 605.

Compliance mit Federal Desktop Core Configuration (FDCC)-Standards

LANDesk Security Suite bietet jetzt erweiterte Unterstützung für die Federal Desktop Core Configuration (FDCC)-Initiative. LANDesk Softwareprodukte wurden vom National Institute of Standards and Technology (NIST) als mit den Security Content Automation Protocol (SCAP)-Standards konform zertifiziert und sind als validierte Produkte auf der Website "National Vulnerability Database" aufgeführt.

Um FDCC-Sicherheitsscan- und -Reparaturtasks ausführen zu können, müssen Sie über ein LANDesk Security Suite Inhaltsabonnement verfügen, mit dem Sie FDCC-spezifische Inhalte herunterladen können. Hierzu gehören: FDCC-Scannererkennung und -installation; FDCC Compliance-Scan und Erstellung von Statusberichten zur Compliance; FDCC-zertifizierter Scan auf Anfälligkeiten und Reparatur nach Komponente.

Mit dem FDCC-zertifizierten Scanner und Sicherheitsinhalt können Sie Ihre verwalteten Geräte scannen, um sicherzustellen, dass diese den FDCC-Standards und -Anforderungen entsprechen.

Nähere Informationen zur Verwendung des FDCC-Scanners und -Sicherheitsinhalts finden Sie unter "Compliance mit den FDCC-Standards – Übersicht" auf Seite 648.

Sicherheitsaktivität

Mit dem Extra "Sicherheitsaktivität" können Sie kritische Aktivitäts- und Statusinformationen für mehrere Sicherheitskomponenten und -dienste anzeigen. Sicherheitsaktivität bietet Ihnen in einem einzigen Extra-Fenster Einblick in die Ergebnisse von LANDesk Antivirusscans, HIPS-Verhinderungen, LANDesk Firewallverhinderungen, verweigerte Geräte und mehr.

Weitere Informationen finden Sie unter "Sicherheitsaktivität" auf Seite 706.

Agenteneinstellungen

Mit dem Extra "Agenteneinstellungen" können Sie Einstellungsdateien für mehrere Sicherheitskomponenten und -dienste erstellen und verwalten. Konfigurationen (d. h. die Dateien mit den entsprechenden Einstellungen) steuern, wie Sicherheitsdienste auf verwalteten Geräten ausgeführt werden.

Mit dem Extra "Agenteneinstellungen" können Sie Sicherheitsagenten bzw. -dienste und zugehörige Einstellungen im Rahmen der anfänglichen Agentenkonfiguration für Ihre verwalteten Geräte bereitstellen, als separate Installations- oder Updatetasks und als Einstellungsänderungstasks.

Weitere Informationen finden Sie unter "Sicherheitskonfigurationen" auf Seite 692.

Endpunktsicherheit

Das Extra "Endpunktsicherheit" schützt Ihre verwalteten Geräte vor Zero-Day-Angriffen, Firewallangriffen, unerlaubten Aktionen und unzulässigem Verhalten von Anwendungen und Prozessen sowie nicht autorisierten Netzwerk- und Geräteverbindungen.

Endpunktsicherheit umfasst benutzerdefinierte Einstellungsdateien (d. h. gespeicherte Konfigurationen für Funktionen und Optionen, die für Zielgeräte bereitgestellt werden können) für die folgenden Sicherheitskomponenten:

- Standorterkennung (Netzwerkverbindungssteuerung über vertrauenswürdige Speicherorte)
- Host Intrusion Prevention System (HIPS)
- LANDesk Firewall
- Gerätesteuerung
- Listen der vertrauenswürdigen Dateien

Host Intrusion Prevention System (HIPS)

LANDesk Host Intrusion Prevention System (HIPS) erweitert die Sicherheitsposition Ihrer Umgebung um ein Sicherheitssystem, das Systeme und Anwendungen proaktiv vor Zero-Day-Angriffen (d. h. bösartigem, nicht autorisiertem Verhalten) schützt. Mittels angepasster Regeln und Dateizertifizierungen überwacht HIPS fortlaufend bestimmte Prozesse, Dateien, Anwendungen und Registrierungsschlüssel und blockiert verbotene Aktionen und Verhalten. Mit HIPS entscheiden Sie selbst, welche Anwendungen auf welche Weise auf Geräten ausgeführt werden dürfen. HIPS versetzt Sie in die Lage, das Dateisystem, die Registrierung und den Systemstart zu schützen und sogar maskierte Rootkits aufzudecken.

Da es sich bei HIPS um ein regelbasiertes und nicht um ein definitionsbasiertes (d. h. signaturbasiertes) System handelt, wie bekannte Anfälligkeits-, Spyware- und Antivirusscans, sind keine ständigen Dateiupdates erforderlich. Die Konfiguration und Bereitstellung der von Ihnen benötigte Ebene der Systemsicherheit nehmen Sie entsprechend Ihren spezifischen Anforderungen vor.

Weitere Informationen finden Sie unter "Host Intrusion Prevention System (HIPS) – Übersicht" auf Seite 719.

LANDesk Firewall

Mit LANDesk Firewall können Sie proprietäre Firewalleinstellungen erstellen und konfigurieren, um Ihre verwalteten Geräte vor nicht autorisiertem Anwendungsverhalten zu schützen.

WICHTIG: Kompatibilität von LANDesk Firewall und Windows-Firewall
Die LANDesk Firewall ergänzt die Windows-Firewall. Beide Firewalls können gleichzeitig auf verwalteten Geräten aktiviert und ausgeführt werden.

Weitere Informationen finden Sie unter "Konfigurieren der LANDesk Firewalleinstellungen" auf Seite 734.

Gerätesteuerung

Die Gerätesteuerung erweitert die Sicherheit Ihres LANDesk Netzwerks um eine zusätzliche Ebene, indem Sie die Möglichkeit erhalten, den Zugriff auf verwaltete Geräte über E/A-Geräte zu überwachen und einzuschränken. Mit der Gerätesteuerung können Sie die Nutzung von Geräten beschränken, die einen Datenzugriff auf das Gerät gestatten, wie z. B. Ports, Modems, Laufwerke, USB-Geräte und Wirelessverbindungen.

Weitere Informationen finden Sie unter "Gerätesteuerung – Übersicht" auf Seite 740.

LANDesk Antivirus

Mit LANDesk Antivirus können Sie Ihr gesamtes verwaltetes Gerätearsenal vor den neuesten bekannten Viren sowie vor vermeintlichen Infektionen schützen. Antivirusscans können (über eine erweiterte Datenbank) auch dazu verwendet werden, Geräte auf Riskware zu prüfen. LANDesk Antivirus ist ein konfigurierbares Tool für den Virenschutz, das nahtlos in LANDesk Security Suite und LANDesk Management Suite integriert ist.

LANDesk Antivirus bietet ein breites Spektrum an Antivirus-Funktionen, das u. a. Folgendes einschließt: Geplante Antivirusscans, On-Demand-Scans, Red-Button-Scans, Datei- und E-Mail-Schutz in Echtzeit, automatischer Download von Virendefinitionsdatei-Updates (die Virensignatur-Datenbank von LANDesk enthält die neuesten bekannten Definitionen und wird mehrmals am Tag aktualisiert), Konfiguration des Verhaltens von Antivirusscans und Endanwenderoptionen, Scanausschlüsse sowie Antivirus-Alarmmeldungen und Berichte.

Zusätzlich können Sie Antivirus-Informationen in Echtzeit für gescannte Geräte sowohl in der Hauptkonsole als auch im Executive Dashboard der Webkonsole anzeigen, um Virenausbrüche gezielt zu identifizieren und die Viruskontrolle während eines festgelegten Zeitraums anzuzeigen.

Weitere Informationen finden Sie unter "LANDesk Antivirus" auf Seite 751.

LANDesk 802.1X NAC

Network Access Control (NAC) verwenden Sie, um Compliance-Sicherheit in Ihrem Netzwerk zu implementieren. Die LANDesk 802.1X NAC-Unterstützung ist so ausgelegt, dass sie die Sicherheit einer vorhandenen 802.1X Radius-Serverimplementierung in Ihrem Netzwerk durch Authentifizierung und Compliance ergänzt.

LANDesk 802.1X NAC gibt Ihnen die Möglichkeit, mithilfe des Extras "Patch und Compliance" benutzerdefinierte Sicherheitskonformitätsrichtlinien zu konfigurieren und mithilfe eines Posture-Validierungsprozesses dafür zu sorgen, dass diese Richtlinien auf Geräten, die eine Verbindung mit Ihrem Netzwerk herstellen möchten, durchgesetzt werden. Fehlerfreie Geräte ("healthy devices") erhalten Zugriff, während fehlerhafte Geräte ("unhealthy devices") in einem Quarantänebereich isoliert und repariert werden und dann entweder vollständigen oder eingeschränkten Netzwerkzugriff erhalten. Sie haben außerdem die Möglichkeit, konformitätsspezifische Sicherheitsscans zu erstellen und zu konfigurieren, die zurzeit verbundene Geräte auf Konformität mit Ihrer Sicherheitsrichtlinie scannt. Vollständige Compliance-Sicherheitsscans können auch von einem Antivirusscan initiiert werden, wenn ein Virus weder unter Quarantäne gestellt noch entfernt werden kann.

WICHTIG: LANDesk NAC erfordert die Einrichtung zusätzlicher Hardware und Software und solide Kenntnisse in den Bereichen 802.1X Radius-Serverkonfiguration, 802.1X-Authentifizierung und Health Posture-Validierung sowie Erfahrung mit anspruchsvolleren Netzwerkinfrastruktur-Design- und Administrationsaufgaben.

Nähere Informationen finden Sie unter "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543.

LANDesk Datenschutz mit Credant

Häufig verwendete LANDesk Extras, die in Security Suite enthalten sind

Gemeinsame LANDesk Extras stellen die grundlegenden Gerätekonfigurations- und Verwaltungskapazitäten sowohl in Management Suite als auch in Security Suite zur Verfügung. Die im Folgenden beschriebenen Extras sind in einer LANDesk Security Suite-Implementierung verfügbar und werden im Menü **Extras** der Hauptkonsole angezeigt.

WICHTIG: Beachten Sie, dass für einige dieser gemeinsamen Extras in einer LANDesk Security Suite-Lizenzaktivierung Beschränkungen gelten.

Agentenkonfiguration

Die Agentenkonfiguration verwenden Sie, um benutzerdefinierte Agentenkonfigurationen für die Bereitstellung und Installation der LANDesk Agenten zu erstellen, die Sie benötigen, um Ihre Netzwerkgeräte zu verwalten und zu schützen. Bei diesen Agenten handelt es sich um den standardmäßigen LANDesk Agenten (einschließlich Inventarscanner, Local Scheduler, Bandbreitenerkennung und Sicherheitsscanner), den Softwareverteilungsagenten und den Softwarelizenzüberwachungsagenten (für die Anwendungsblockierung).

HINWEIS: Agenten, die nicht für LANDesk Security Suite relevant sind
Die folgenden LANDesk-Agenten (Komponenten) sind in einer Security Suite-Installation NICHT relevant:
– Benutzerdefinierte Datenformulare
– Remotesteuerung
– Betriebssystembereitstellung

Berichte

Das Extra "Berichte" verwenden Sie für die Erstellung und Veröffentlichung eines breiten Spektrums von Spezialberichten, die nützliche Informationen zu verwalteten Geräten bereitstellen, einschließlich mehrerer vordefinierter Patch und Compliance-, Antivirus- und LANDesk NAC-Compliance-Berichte.

HINWEIS: Berichte, die nicht für LANDesk Security Suite relevant sind
Die folgenden Berichtkategorien sind NICHT für Security Suite relevant: Alle Inventarberichte, alle SLM-Berichte und alle Remotesteuerungsberichte.)

Geplante Tasks

"Geplante Tasks" verwenden Sie, um wiederkehrende Tasks zu erstellen, die sich speziell auf die Sicherheits- und Patchverwaltung, Reparatur, Erzwingung der Sicherheitskonformität, Virenschutzscans usw. beziehen. Sie können die Zielgeräte und Zeitplanoptionen des Tasks konfigurieren.

HINWEIS: Geplante Tasks, die nicht für LANDesk Security Suite relevant sind
Die folgenden geplanten Tasks (Skripte) sind NICHT für Security Suite relevant: Benutzerdefinierte Datenformulare, benutzerdefinierte Skripte, Handheld-Tasks und OSD-Skripte. Die Taskoptionen für Verteilungspakete und Liefermethoden lassen sich in Security Suite ebenfalls nicht konfigurieren.)

Erkennung nicht verwalteter Geräte

Die Funktion "Erkennung nicht verwalteter Geräte" verwenden Sie, um Geräte in Ihrem Netzwerk zu finden, die noch keinen Inventarscan an die Coredatenbank gesendet haben.

Die erweiterte Geräteerkennung (XDD) arbeitet außerhalb der normalen scanbasierten Erkennungsmethoden, die von UDD eingesetzt werden. Verwaltete Geräte, auf denen der Agent für die erweiterte Geräteerkennung installiert ist, hören ARP (Address Resolution Protocol)-Broadcasts ab und legen einen Zwischenspeicher mit Geräten an (sowohl im Hauptspeicher als auch in einer Datei auf dem lokalen Laufwerk), die diese Broadcasts erzeugen. Die erweiterte Geräteerkennung kann auch WAP (Wireless Access Point)-Geräte erkennen.

Rollenbasierte Administration

Mit dem Extra "Benutzerverwaltung" können Sie den Security Suite-Verwaltungsrollen Benutzer zuordnen und deren Zugriff auf spezifische Extras und verwaltete Geräte auf der Basis ihrer administrativen Rolle erteilen.

In der rollenbasierten Administration bestimmen Sie durch die Zuweisung von Rollen (und den zugehörigen Rechten), welche Tasks ein Benutzer ausführen kann, und mit Bereichen (deren Zuweisung auf der Basis von Gerätegruppen, Abfragen, LDAP-Verzeichnissen oder benutzerdefinierten Verzeichnissen erfolgt), welche Geräte ein Benutzer anzeigen und verwalten kann. In Security Suite stehen folgende Rollen zur Verfügung: Patch und Compliance, Network Access Control, Agenteneinstellungen, Softwareverteilung, Verwaltung öffentlicher Abfragen und Erkennung nicht verwalteter Geräte.

HINWEIS: Rollen und Rechte, die nicht für LANDesk Security Suite relevant sind
Die folgenden Rechte der rollenbasierten Administration sind NICHT für Security Suite relevant: Betriebssystembereitstellung, Remotesteuerung, Assetkonfiguration, Assetdateneintrag und Softwarelizenzüberwachung.

Lokale Konten

Das Tool "Lokale Konten" ist ein Verwaltungswerkzeug, das dazu dient, die Benutzer und Gruppen auf lokalen Rechnern in Ihrem Netzwerk zu verwalten. Sie können von der Konsole aus Benutzer und Gruppen hinzufügen und löschen, Benutzer in Gruppen einfügen oder aus Gruppen löschen, Kennwörter einrichten und ändern, Benutzer- und Gruppeneinstellungen bearbeiten und Tasks zum Zurücksetzen von Kennwörtern für mehrere Geräte erstellen.

Sonstige in Security Suite enthaltene LANDesk Management Suite-Funktionen

Zusätzlich zu den oben aufgeführten Tools aus dem Menü "Extras" der Konsole stellt Security Suite folgende LANDesk Funktionen zur Verfügung:

- Windows-Konsole, zusätzliche Konsolen, Webkonsole
- Benutzerdefinierte Konsolenlayouts
- Netzwerkansicht für verwaltete Geräte und Abfragen
- Startmenüs für verwaltete Geräte und Abfragen
- Dienstekonfiguration
- Inventar
- Datenbankabfragen
- Softwareverteilung
- Softwarelizenzüberwachung
- Alarmfunktion
- Inhaltsreplikation und bevorzugte Server

WICHTIG: Benutzerdefinierte Datenformulare werden in LANDesk Security Suite nicht unterstützt
Benutzerdefinierte Datenformulare werden mit einer reinen LANDesk Security Suite-Lizenz nicht zur

Verfügung gestellt. Sie müssen im Besitz einer LANDesk Management Suite Volllizenz sein, um die benutzerdefinierten Formulare verwenden zu können.

Zusätzliche Informationsquellen

Die übrigen verknüpften Hilfethemen finden Sie im Anschluss an die Hilfethemen zum Sicherheitsextra in den Abschnitten der LANDesk Management Suite-Hilfe, die sich mit den zuvor erwähnten LANDesk Extras befassen (einschließlich der grundlegenden Erläuterungen zur Verwendung der Konsole und der Netzwerkansicht).

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter LANDesk Benutzercommunity – Startseite

Verwandte Themen

"Einführung in LANDesk Security Suite" auf Seite 526

Netzwerkzugriffskontrolle (Network Access Control)

LANDesk NAC – Übersicht

Network Access Control (NAC) ist eine zentrale Komponente einer umfassenden Sicherheitsverwaltungslösung. NAC schützt Ihr Netzwerk vor unbefugten Zugriffen, destruktiven Manipulationen sowie externen Sicherheitslücken, die durch anfällige oder fehlerhafte Geräte verursacht wurden und die Ihr Netzwerk infizieren und schädigen können.

LANDesk Security Suite bietet ein 802.1X NAC-Extra, das die Sicherheit einer vorhandenen 802.1X Radius-Serverimplementierung in Ihrem Netzwerk unterstützt und erweitert. LANDesk 802.1X NAC ergänzt die von 802.1X bereitgestellte, einfache Zugriffssteuerung durch Funktionen zur Authentifizierung und Compliance.

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter http://community.landesk.com

Die Network Access Control (NAC)-Lösung erweitert Ihr Netzwerk um eine zusätzliche Sicherheitsebene, indem sie es Ihnen ermöglicht, anfälligen oder beschädigten Geräten den Zugriff auf das Netzwerk zu verweigern und kritische Netzwerkressourcen vor Systemen, die eine Verbindung hergestellt haben und beschädigt wurden, zu schützen.

NAC setzt die Endpunkt-Perimetersicherheit mithilfe von Sicherheitstechnologien und -systemen nach dem Industriestandard durch. Network Access Control bietet Flexibilität bei der Implementierung der NAC-Funktionalität in Ihrem Netzwerk, da branchenübliche Standards und Methodologien wie beispielsweise IEEE 802.1X unterstützt werden.

Network Access Control ermöglicht es Ihnen, benutzerdefinierte Baseline-Sicherheitsrichtlinien zu definieren, Geräte (verwaltete und nicht verwaltete) auf die Einhaltung von Sicherheitsrichtlinien zu scannen, den Zustand (Posture) von Geräten, die eine Verbindung mit dem Netzwerk herstellen möchten, zu überprüfen und den Zugriff auf kritische Netzwerkressourcen davon abhängig zu machen, ob das Gerät "compliant" ist (d. h. die von Ihnen definierten Sicherheitsrichtlinien erfüllt). Fehlerfreie Geräte erhalten uneingeschränkten Netzwerkzugriff. Wenn ein Gerät als fehlerhaft erkannt wird, erhält es keinen Zugriff auf das Netzwerk; stattdessen wird es in einem virtuellen Quarantänebereich isoliert, in dem es entweder mit den Wartungsfunktionen von Security Suite repariert werden kann oder limitierten Netzwerkzugriff erhält.

Mithilfe von NAC können Sie die Sicherheitsinformationen eines Geräts durch einen Vergleich mit benutzerdefinierten Sicherheitsrichtlinien analysieren, sobald es versucht, auf Ihr Netzwerk zuzugreifen. Darüber hinaus können Sie den Sicherheitszustand von Geräten, mit denen bereits eine Verbindung besteht, überwachen, Netzwerkzugriff erteilen oder verweigern, Geräte, die die Anforderungen der Sicherheitsrichtlinien nicht erfüllen, in einem Quarantänebereich isolieren sowie anfällige Geräte reparieren, damit diese erneut auf Konformität mit Sicherheitsrichtlinien gescannt werden können und Zugriff auf das Netzwerk erhalten, sobald sie als fehlerfrei gelten.

Vorteile und Funktionen von Network Access Control

Sie können mit NAC folgendes erreichen:

- Erstellen und Durchsetzen von benutzerdefinierten Compliance-Sicherheitsrichtlinien
- Implementieren einer zuverlässigen Lösung für die Unternehmenssicherheit, die rund um die Uhr im Einsatz ist
- Bewerten der Sicherheitsinformationen (des Systemzustands) von Geräten, die versuchen, eine Verbindung herzustellen
- Verhindern, dass infizierte oder beschädigte Systeme auf das Netzwerk zugreifen
- Isolieren nicht sicherheitskonformer Geräte in einem geschützten Bereich
- Reparieren infizierter Geräte, um sie sicherheitskonform zu machen
- Reduzieren von Ausfallzeiten infolge bösartiger Übergriffe
- Schutz Ihres Netzwerks, Ihrer Systeme, Anwendungen und Daten vor externen Bedrohungen
- Erweitern vorhandener Sicherheitstechnologien und Standards

Compliance-Sicherheitsrichtlinien

Compliance-Sicherheitsrichtlinien bestehen aus Regeln, die den Zustand eines Geräts überprüfen, indem sie es auf Anfälligkeiten (in Form von fehlenden oder veralteten Betriebssystem- und Anwendungs-Patches), Softwareupdates, Virenschutz-Engine- und Signaturdateien, Firewall-Präsenz und -Einstellungen sowie Spyware kontrollieren.

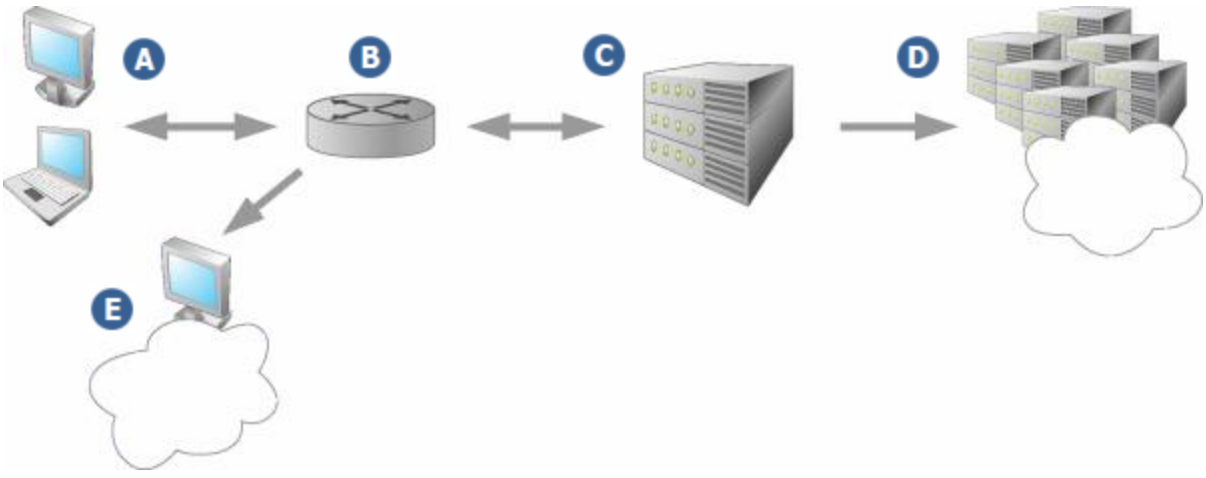
Weitere Informationen zum Definieren einer Compliance-Sicherheitsrichtlinie im Extra "Patch und Compliance" in der Konsole finden Sie unter "Definieren von Compliance-Sicherheitskriterien im Extra "Patch und Compliance"" auf Seite 564.

Die grundlegenden Komponenten von NAC

Die folgenden Abschnitte beschreiben die wichtigsten Komponenten einer NAC (Network Access Control)-Implementierung, die Funktion der jeweiligen Komponente und ihr Zusammenspiel.

NAC-Hauptkomponenten und Prozessablauf

Das nachstehende Diagramm zeigt die NAC-Hauptkomponenten, deren Funktion und den Kommunikationsfluss zwischen den verschiedenen Komponenten.



***A** Geräte, die versuchen, auf das Netzwerk zuzugreifen, **B** Gerät für die Netzwerkzugriffssteuerung, **C** Entscheidungspunkt für Netzwerkzugriff / Richtlinienserver, **D** Unternehmensnetzwerk, **E** Quarantäne-VLAN*

Beschreibung der grundlegenden NAC-Komponenten

Komponente	Beschreibung
A: Geräte, die versuchen, auf das Netzwerk zuzugreifen	Hierzu gehören mobile Laptops oder Laptops, die nur gelegentlich Verbindungen mit dem Netzwerk herstellen, Mitarbeiter von Vertragsunternehmen und Gastbenutzer sowie reguläre Netzwerkbenutzer, die versuchen, auf das Netzwerk zuzugreifen. Geräte mit installiertem Trust-Agenten können mit dem Richtlinienserver oder Posture Validation-Server kommunizieren, um Informationen zum Gerätezustand zu senden und zu empfangen; diese Geräte können darüber hinaus vom Wartungsserver repariert werden, wenn während des Sicherheitsscans Anfälligkeiten erkannt werden. Geräte ohne Trust-Agenten können weder mit dem Posture Validation-Server kommunizieren noch repariert werden. Wenn ein Gerät, auf dem kein Trust-Agent installiert ist, zum ersten Mal gescannt wird, erfolgt eine Umleitung des Geräts zu einer Webseite, auf der sich Verknüpfungen zum Installieren des relevanten Trust-Agenten befinden.
B: Gerät für die Netzwerkzugriffsteuerung	Das Gerät für die Netzwerkzugriffsteuerung dient als Netzwerkgerät des "ersten Hop" von der Geräteperspektive aus; es initiiert die Zustandsprüfung und den Authentifizierungsprozess.
C: Richtlinienserver / Posture Validation-Server (Netzwerkzugriff-Entscheidungspunkt)	Ein fest zugeordneter Backend-Server, auch Posture Validation-Server genannt, der die Zustandsinformationen (den Status) von Geräten, die Zugriff anfordern, auf der Basis der Compliance-Regeln (Sicherheitsrichtlinie) auswertet, die vom Coreserver aus auf dem Posture-Validierungsserver veröffentlicht werden. Übermittelt eine den Zustand betreffende Antwort (fehlerfrei, fehlerhaft etc.) über das Netzwerkzugriffssteuerungsgerät.
D: Unternehmensnetzwerk	Kritischer Netzwerkbereich und Ressourcenbestand, der von NAC vor fehlerhaften, infizierten oder anderen anfälligen Geräten geschützt wird.
E: Quarantäne-VLAN	Virtueller geschützter Netzwerkbereich, in dem nicht sicherheitskonforme Geräte isoliert und entweder repariert, erneut gescannt und dann mit allen Zugriffsrechten für das Unternehmensnetzwerk ausgestattet oder mit eingeschränktem Zugriff auf Netzwerkressourcen, z. B. das Internet, zurückbehalten werden.

NAC-Voraussetzungen und RBA-Rechte

Für die Verwendung der NAC-Funktion müssen Sie im Besitz einer gültigen Security Suite-Lizenz sein (Coreserver-Aktivierung).

Für den Download der Definitionen für Anfälligkeiten, Systemkonfigurationsbedrohungen, Spywaredefinitionen und Virusmusterdateien, die zum Erstellen von benutzerdefinierten Compliance-Sicherheitsrichtlinien verwendet werden, ist NAC nicht nur auf die Scanning- und Reparaturfunktionen des Extras "Patch und Compliance" angewiesen, sondern auch auf die Security Suite-Inhaltsabonnements.

Eine Gruppe mit der Bezeichnung "Compliance" wurde zur Strukturansicht des Extras "Patch und Compliance" hinzugefügt. Benutzer, die über das "Patch und Compliance"-Recht verfügen, können Sicherheitstypdefinitionen zur Gruppe "Compliance" hinzufügen und daraus entfernen. Die in der Gruppe "Compliance" enthaltenen Sicherheitsdefinitionen schließen die Compliance-Sicherheitsrichtlinie ein und werden auf Geräten gesucht, die versuchen, eine Verbindung herzustellen, damit der Systemzustand dieser Geräte bestimmt werden kann.

Rollenbasierte Administration mit LANDesk 802.1X NAC

Network Access Control stützt sich auf folgende rollenbasierte Rechte:

Das Recht "Patch und Compliance"

Dieses Recht ist für die Anzeige und den Zugriff auf das Extra "Patch und Compliance" und für den Download von Updates für Sicherheitsinhalte erforderlich, die zum Definieren von Complianceregeln benötigt werden. Dieses Recht wird zum Hinzufügen oder Entfernen von Sicherheitsdefinitionen aus der Compliance-Gruppe benötigt.

Das Administratorrecht

Dieses Recht wird benötigt, um Geräte mit Trust-Agents für das Compliance-Scanning zu konfigurieren und NAC-Services in der Konsole einzurichten.

HINWEIS: Das LANDesk Administrator-Recht beinhaltet automatisch alle Rechte, einschließlich der zwei weiter oben erwähnten Sicherheitsrechte.

Schnellstart-Aufgabenliste für LANDesk 802.1X NAC

Diese Aufgabenliste können Sie als Hilfsmittel bei der Durchführung der Planungs-, Einrichtungs- und Konfigurationsaufgaben verwenden, die zur Implementierung der 802.1X NAC-Unterstützung in Ihrem Netzwerk erforderlich sind.

Sie können diese Aufgabenliste drucken und als Orientierungshilfe bei der Durchführung der einzelnen Schritte des Implementierungsvorgangs verwenden. Wenn Sie diese Aufgabenliste online geöffnet haben, klicken Sie auf **Weitere Informationen**, um ausführliche Hinweise für eine bestimmte Aufgabe anzuzeigen.

Fertig	Aufgabe	Weitere Informationen erhalten Sie unter
	Voraussetzung: In Ihrem Netzwerk muss ein Coreserver installiert und in Betrieb sein, der über eine aktivierte Security Suite Lizenz und Abonnements für Sicherheitsinhalte verfügt.	Informationen zur Verwendung des Extras "Patch und Compliance" finden Sie unter "Patch und Compliance" auf Seite 578.

Fertig	Aufgabe	Weitere Informationen erhalten Sie unter
	• Installieren Sie den Coreserver. • Aktivieren Sie den Core mit einer Security Suite-Lizenz. • Melden Sie sich als Benutzer mit Administratorrechten oder als Benutzer mit dem Recht "Sicherheit" an (gestattet den Download von Sicherheitsinhalten und das Kopieren derselben in die Compliance-Gruppe).	Informationen über die 802.1X NAC-Komponenten und den Prozessablauf finden Sie unter "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543. Informationen über die Netzwerktopologie und Überlegungen zum Design einer 802.1X NAC-Implementierung finden Sie unter "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543.
	Richten Sie einen Wartungsserver ein: • Auf einem separaten Servercomputer: • Führen Sie das CONFIGURE.REMEDIATION.SERVER.VBS-Setup-Skript aus, das sich an folgender Position befindet: <Coreserver>\LDMain\Install\TrustedAccess\RemediationServer • **HINWEIS:** Das Skript konfiguriert den Server automatisch für die Durchführung von Reparaturen durch: • Erstellen einer Webfreigabe mit dem Namen LDLogon (normalerweise unter: c:\inetpub\wwwroot\LDLogon) • Ermöglichen des anonymen Zugriffs auf die LDLogon-Freigabe mit Lese- und Navigationsrechten • Hinzufügen eines neuen MIME-Typs für .LRD-Dateien und Festlegen auf application/octet-stream.	"Einrichten und Konfigurieren eines Wartungsservers" auf Seite 559
	Konfigurieren Sie den Wartungsserver in der Konsole (durch Hinzufügen): • Klicken Sie mit der rechten Maustaste in **Network Access Control** auf **802.1X**, klicken Sie dann auf **802.1X konfigurieren**, dann auf **Wartungsserver** und schließlich auf **Hinzufügen**. • Geben Sie die IP-Adresse des Wartungsservers ein und den UNC-Pfad zu der LDLogon-Webfreigabe, die Sie auf dem Wartungsserver erstellt haben, in der Dateien veröffentlicht werden, und geben Sie auch die Benutzeranmeldeinformationen ein und klicken Sie dann auf **OK**.	"Einrichten und Konfigurieren eines Wartungsservers" auf Seite 559
	Veröffentlichen Sie die NAC-Einstellungen für Wartungsserver:	"Veröffentlichen von NAC-Einstellungen

Fertig	Aufgabe	Weitere Informationen erhalten Sie unter
	• Klicken Sie in **Network Access Control** mit der rechten Maustaste auf **802.1X**, klicken Sie auf **NAC-Einstellungen veröffentlichen**, wählen Sie **Alle** aus und klicken Sie dann auf **OK**. • **HINWEIS:** Die erste Veröffentlichung muss ALLE der NAC-Einstellungen einschließen; nachfolgende Veröffentlichungen können nur Compliance-Inhalt enthalten.	für Server" auf Seite 566
	Definieren Sie Compliance-Sicherheitskriterien im Extra "Patch und Compliance": • Im Extra **Patch und Compliance** der Konsole: • Laden Sie die Sicherheitsinhaltsdefinitionen und Patches herunter. • Fügen Sie der **Compliance**-Gruppe Sicherheitsdefinitionen hinzu, um Ihre Compliance-Sicherheitsrichtlinie zu definieren. • Stellen Sie sicher, dass hiermit verknüpfte Patches gedownloadet werden und bereitgestellt werden können. • Erstellen Sie eine Compliance-Einstellung die 802.1X-unterstütztes Scannen durchsetzt. • (Die 802.1X NAC-Compliance-Sicherheitsrichtlinie wird außerdem durch die automatische Quarantänezeiteinstellung in der Geräteagentenkonfiguration definiert.)	"Definieren von Compliance-Sicherheitskriterien im Extra "Patch und Compliance"" auf Seite 564
	Aktivieren Sie die 802.1X NAC-Unterstützung und konfigurieren Sie den 802.1X-Radius-Server oder -Proxy in der Konsole: • Klicken Sie in **Network Access Control** mit der rechten Maustaste auf **802.1X**, klicken Sie auf **802.1X konfigurieren**, klicken Sie auf **Radius-Server**, nachdem Sie sich vergewissert haben, dass die Option **802.1X-Radius-Server aktivieren** markiert ist, und wählen Sie dann entweder das LTA EAP IAS-Plugin oder den LTA Radius-Proxy aus (erfordert die Konfiguration von Proxy-Einstellungen).	"Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543
	Installieren Sie den LANDesk 802.1X-Agenten auf verwalteten Geräten zur Aktivierung des Compliancescans: (**HINWEIS:** Bei der Bereitstellung des 802.1X-Agenten müssen Sie die Adressierungsmethode des Quarantänenetzwerks für fehlerbehaftete Geräte angeben. Die Quarantäneadressierung kann über einen selbstzugewiesenen IP-Adressbereich oder über DHCP im Quarantänenetzwerk erfolgen. Sie konfigurieren dieses Adressierungsschema auf dem Router. • **Für verwaltete Mitarbeitergeräte:** Falls der Standard LANDesk Agent bereits vorhanden ist, aktivieren Sie die 802.1X-Unterstützung mit einer neuen Geräte-Agentenkonfiguration. Oder, falls kein Standardagent vorhanden ist, aktivieren Sie die 802.1X-Unterstützung mit der ersten Agentenkonfiguration. Oder aktivieren Sie die 802.1X-Unterstützung mit einer Agentenkonfiguration auf Geräte in UDD.	"Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543

Fertig	Aufgabe	Weitere Informationen erhalten Sie unter
	• **Für nicht verwaltete Mitarbeitergeräte:** Aktivieren Sie die 802.1X-Unterstützung mit einer Pullinstallation des Standardagenten (wscfg32.exe) oder mit einer unabhängigen Agentenkonfiguration.	
	Konfigurieren Sie Ihren Netzwerkswitch für 802.1X-Authentifizierung, Quarantäne und Reparatur: • Gehen Sie auf die Support-Website für Empfehlungen und Beispielkonfigurationen.	"Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543
	Konfigurieren Sie Ihren Netzwerkrouter so, dass die Sicherheit zwischen dem Produktionsnetzwerk und dem 802.1X-Quarantänenetzwerk gewährleistet ist. • Gehen Sie auf die Support-Website für Empfehlungen und Beispielkonfigurationen.	"Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543
	Vergewissern Sie sich, dass der Authentifizierungsvorgang und der Posture-Validierungsvorgang richtig funktionieren: • Versuchen Sie einen einfachen Test für 802.1X NAC, indem Sie ein mit LANDesk 802.1X NAC-Unterstützung konfiguriertes Gerät mit dem Netz verbinden.	
	Führen Sie fortlaufende Sicherheitsverwaltungsaufgaben im Compliance-Umfeld aus: • Vergewissern Sie sich, dass die 802.1X NAC-Unterstützung aktiviert ist. • Grundlegendes zu den Folgen des Posture-Vorgangs auf Geräten, die eine Verbindung herstellen • Anzeigen von nicht konformen Geräten • Ändern und Aktualisieren von Compliance-Sicherheitsrichtlinien • Hinzufügen nicht verwalteter Geräte • Konfigurieren und Anzeigen der Compliance-Protokollierung	"Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist." auf Seite 572

Zurück zum Haupthilfethema für LANDesk 802.1X NAC gelangen Sie über "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543.

Das Extra "LANDesk 802.1X NAC" – Übersicht

LANDesk 802.1X NAC dient der Steuerung des Netzwerkzugriffs, indem es korrekte Anmeldeinformationen für die Authentifizierung und einen aktiven Standardagenten auf dem Gerät erfordert. Ferner können Sie die Konformität des Gerätezustands mit Ihrer benutzerdefinierter Sicherheitsrichtlinie validieren und fehlerbehaftete Geräte unter Quarantäne stellen und warten.

LANDesk 802.1X NAC arbeitet mit allen wichtigen Switching-Anbietern zusammen, die den 802.1X-Standard unterstützen. Ein 802.1X Radius-Proxy kann in eine vorhandene AAA (Authentication, Authorization und Accounting)-Architektur für die Identitätsverwaltung, die Benutzer und Endpunkte authentifiziert, integriert werden, oder als unabhängiger Radius für Umgebungen fungieren, die nur eine Compliance-Überprüfung für den Endpunkt erfordern. Radius Proxy ermöglicht Switch-Port-Zugriff abhängig von den Authentifizierungsergebnissen für angeschlossene Endpunkte.

In den folgenden Abschnitten erfahren Sie, wie die LANDesk 802.1X NAC-Unterstützung in einer bestehenden NAC-Umgebung (NAC, Network Access Control) geplant, eingerichtet, konfiguriert und aktiviert wird.

Aufgabe des Extras LANDesk 802.1X NAC ist es, die Sicherheit einer vorhandenen 802.1X Radius-Serverimplementierung in Ihrem Netzwerk zu unterstützen und zu erweitern. LANDesk 802.1X NAC ergänzt die von 802.1X bereitgestellte, einfache Zugriffssteuerung durch Funktionen zur Authentifizierung und Compliance.

WICHTIG: Vorausgesetztes technisches Wissen und Know-how zum Einrichten von NAC
Beachten Sie, dass NAC zusätzliche Hardware- und Softwarekonfiguration über die grundlegende Coreserver-Installation hinaus erfordert. Aufgrund der technischen Anforderungen dieser zusätzlichen Setup-Arbeit geht LANDesk davon aus, dass Sie mit der 802.1X Radius-Serverkonfiguration, 802.1X-Authentifizierung und Health Posture-Validierung vertraut sind und anspruchsvollere Netzwerkinfrastruktur-Design- und Administrationsaufgaben ausführen können.

Welche Schritte Sie nach dem Einrichten der LANDesk 802.1X NAC-Unterstützung ausführen sollten

Nachdem Sie die Einrichtungstasks für die LANDesk 802.1X NAC-Unterstützung abgeschlossen haben, bestehen die nächsten Schritte der NAC-Implementierung darin, die Compliance-Sicherheitsrichtlinie zu definieren, die NAC-Einstellungen für die entsprechenden Server zu veröffentlichen und die HTML-Reparaturseiten bei Bedarf anzupassen. Weitere Informationen zur Durchführung dieser Tasks finden Sie unter "Definieren von Compliance-Sicherheitskriterien im Extra "Patch und Compliance"" auf Seite 564.

Weitere fortlaufenden NAC-Verwaltungsaufgaben sind: Sicherstellen, dass die 802.1X NAC-Dienste aktiviert sind, Verwenden der Option zum Gewähren/Einschränken des Zugriffs für jedermann, Verstehen, was geschieht, wenn die "Posture" (der Zustand) verbundener Geräte evaluiert wird, Aktualisieren der Compliance-Sicherheitsregeln und -richtlinien und erneutes Veröffentlichen von NAC-Einstellungen, Hinzufügen nicht verwalteter Geräte zum Extra für die Erkennung nicht verwalteter Geräte, Anzeigen betroffener Geräte und Konfigurieren der Protokollierung. Nähere Informationen finden Sie unter "Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist." auf Seite 572.

Schnellstartliste als Referenz

Diese Aufgaben-Checkliste können Sie als Orientierungshilfe bei der Ausführung der Schritte zum Einrichten einer LANDesk 802.1X NAC-Lösung verwenden. Siehe "Schnellstart-Aufgabenliste für LANDesk 802.1X NAC" auf Seite 540.

LANDesk 802.1X NAC-Technologien

802.1X ist ein IEEE-Sicherheitsprotokoll für die portgestützte Netzwerkzugriffssteuerung. 802.1X bietet Authentifizierung gegenüber Geräten, indem entweder eine Verbindung hergestellt oder der Zugriff verhindert wird, wenn die Authentifizierung fehlschlägt. 802.1X basiert auf EAP (Extensible Authentication Protocol) und seit neuestem auch auf PEAP (Protected Extensible Authentication Protocol). 802.1X wird von den meisten Netzwerkschaltern unterstützt und kann für die Authentifizierung von Clients konfiguriert werden, auf denen Agentensoftware installiert ist.

802.1X NAC ist eine Radius-Proxy-Authentifizierungs- und Netzwerkzugriffstechnologie, die mit allen wichtigen Switching-Anbietern zusammenarbeitet, die den 802.1X-Standard unterstützen. Mit 802.1X NAC führt ein Radius-Server – ein Microsoft IAS-Server mit dem EAP IAS-Plugin oder ein Radius-Server mit dem 802.1X-Proxy – die Posture Validation (Zustandsüberprüfung) aus; anders ausgedrückt: er überprüft die Übereinstimmung mit den Sicherheitsrichtlinien.

Die 802.1X-Standardauthentifizierung erfordert einen Benutzernamen und ein Kennwort für den Zugriff auf das Netzwerk. LANDesk 802.1X NAC erweitert dieses Basismodell, indem zusätzlich vorausgesetzt wird, dass der Standard LANDesk Agent (CBA) auf verwalteten Geräten installiert ist, die Zugriff auf das Netzwerk anfordern, und dass das Antragstellergerät mit Ihren benutzerdefinierten Sicherheitsrichtlinien kompatibel ist. NAC prüft die Anwesenheit des Agenten (CBA), indem es nach einer eindeutigen Gerätekennung sucht, die vom Agenten selbst erstellt wurde. (Hinweis: EAP unternimmt keinen Authentifizierungsversuch, bis die Gerätekennung gefunden wird.)

802.1X NAC mit dem EAP IAS-Plugin verwendet einen eigenen NAC EAP-Agenten, der sowohl auf dem IAS Radius-Server als auch auf den verwalteten Geräten gespeichert ist. Der LTA EAP-Agent ist über eine Agentenkonfiguration auf Ihren verwalteten Geräten installiert.

Um die Netzwerkzugriffssteuerung (NAC) zu implementieren, müssen Sie abgesehen von der spezifischen 802.1X Radius-Serverkomponente und der erforderlichen Switch- und Routerkonfiguration auch einen Wartungsserver einrichten.

Bei der 802.1X Network Access Control fungiert der Radius-Server als Entscheidungspunkt für den Netzwerkzugriff und arbeitet mit dem Netzwerkswitch zusammen. Der Netzwerkswitch dient als Instrument für die Steuerung des Netzwerkzugriffs und leitet Geräteauthentifizierungsanforderungen an den Radius-Server weiter, der dann die eigentliche Authentifizierung durchführt. Abhängig von den Ergebnissen, die vom Radius-Server an den Switch zurückgegeben werden, ermöglicht oder verweigert der Switch den Zugriff auf das Netzwerk.

802.1X NAC-Komponenten, Prozessablauf und Netzwerktopologie

In diesem Abschnitt werden die Komponenten beschrieben, aus denen 802.1X NAC zusammengesetzt ist. Darüber hinaus erfahren Sie in diesem Abschnitt, was passiert, wenn ein Gerät versucht, bei aktiviertem NAC auf das Unternehmensnetzwerk zuzugreifen oder eine Verbindung mit ihm herzustellen.

Die folgenden Komponenten sind für LANDesk 802.1X NAC erforderlich.

Erforderliche Komponenten

Komponente	Beschreibung
Coreserver	Stellt das für die folgenden Aufgaben verwendete Extra "Patch und Compliance" zur Verfügung: Download von Sicherheitsinhalten (wie z. B. Anfälligkeitsdefinitionen für Betriebssysteme und Anwendungen, Spywaredefinitionen usw.) Definition von Compliancekriterien Konfiguration von Wartungsservern Konfiguration von Radius-Proxy-Installationspaketen (MSI-Paketen) Konfiguration und Veröffentlichung von NAC-Einstellungen (einschließlich Compliance-Sicherheitsrichtlinien und Reparaturquellen für das Scannen und Reparieren von Geräten)
Radius-Server-Plugin Oder Radius-Proxy	Dient als Entscheidungspunkt für den Netzwerkzugriff. Das 802.1X IAS-Server-Plugin verwenden Sie, wenn Sie einen vorhandenen IAS-Server verwenden oder einen neuen IAS-Server konfigurieren möchten. Die Radius-Proxymethode verwenden Sie, wenn Sie einen anderen Radius-Server als IAS haben oder wenn Sie PEAP als den spezifizierten EAP-Typ verwenden möchten.
Wartungsserver	Enthält die laut Ihrer Sicherheitsrichtlinie erforderlichen Setup- und Unterstützungsdateien (Sicherheitstypdefinitionen und erforderliche Patches sowie die HTML-Reparaturseiten, die zum Scannen von Geräten auf Anfälligkeiten verwendet werden). Repariert alle erkannten Anfälligkeiten, so dass das Gerät als fehlerfrei oder compliant (konform) gescannt werden kann und daraufhin Netzwerkzugriff erhält.
Switch	Dient als Instrument für die Steuerung des Netzwerkzugriffs und leitet Geräteauthentifizierungsanforderungen an den Radius-Server weiter, der dann die eigentliche Authentifizierung durchführt.
Router	Erfüllt die Funktion eines Netzwerkzugriffsgeräts, das die Einhaltung der Compliance-Sicherheitsrichtlinie erzwingt. Kommuniziert zur Evaluierung der Posture-Informationen des Endpunktgeräts sowohl mit dem Gerät, das den Zugriffsversuch unternimmt, als auch mit dem 802.1X Radius-Server. Anders formuliert: In einer 802.1X NAC-Umgebung erzwingt der Router die Durchsetzung der Richtlinie auf dem Netzwerk und erteilt oder verweigert Zugriffsprivilegien.

Komponente	Beschreibung
Geräte	Benutzergeräte, die versuchen, auf das Netzwerk Ihres Unternehmens zuzugreifen. Typische Endpunktgeräte sind Desktopcomputer und Laptops, aber auch Geräte ohne Client, wie etwa Drucker usw. zählen hierzu. NAC gibt Ihnen die Möglichkeit, den Zustandsstatus dieser Geräte, zu denen Verbindungen hergestellt werden, zu bewerten und den Netzwerkzugriff auf der Basis ihrer Posture-Informationen zu beschränken.

802.1X NAC-Prozessablauf

1. Ein verwaltetes Gerät, das mit dem LANDesk 802.1X-Agenten konfiguriert wurde, unternimmt einen ersten Versuch, auf das Unternehmensnetzwerk zuzugreifen.
2. Der Netzwerk-Switch (konfiguriert für 802.1X-Passthru-Weiterleitung und als Zugriffssteuerungspunkt fungierend) sendet eine EAP-Antragskennung an das Antragstellergerät.
3. Auf dem Gerät erscheint eine Eingabeaufforderung für einen Benutzernamen und ein Kennwort. Der Endanwender muss gültige Anmeldeinformationen eingeben, die vom Switch zusammen mit einem Token, das dem EAP-Antwortpaket hinzugefügt wurde, an den Radius-Server weitergeleitet werden (der entweder mit dem LTA EAP-Plugin oder mit einem LTA-Radius-Proxy konfiguriert wurde und als Zugriffsentscheidungspunkt fungiert).
4. Wenn die zur Authentifizierung angegebenen Anmeldeinformationen erkannt werden und das Token darauf hinweist, dass auf dem Gerät der Standardagent installiert ist, führt LANDesk 802.1X NAC einen Compliance-Sicherheitsscan durch, der die Posture bzw. den Health-Zustand des Geräts entsprechend Ihrer benutzerdefinierten Sicherheitsrichtlinie bestimmt. Der Scan wird von einem Compliance-Scantask durchgeführt, der eine Compliance-Einstellung mit aktivierter Option **802.1X-unterstütztes Scannen durchsetzen** auf der Seite **Compliance** hat.
5. Wird das Gerät als fehlerfrei (sicherheitskonform) eingestuft, erhält es Zugriff auf das Unternehmensnetzwerk.
6. Wenn das Gerät als fehlerhaft (nicht sicherheitskonform) eingestuft wird, verbleibt es im Quarantäne-VLAN. Ein Meldungsfeld informiert den Benutzer, wie er den Wartungsserver kontaktieren kann, um Scans zur Anfälligkeitsbewertung und -reparatur durchzuführen. Der Reparatur-Shortcut wird auf dem Desktop der Geräts erstellt. Der Endbenutzer kann entscheiden, ob das Gerät im Quarantäne-VLAN bleiben soll, oder er kann die erforderlichen Maßnahmen ergreifen, die belegen, dass das Gerät die Sicherheitsrichtlinie des Netzwerks erfüllt, und auf diese Weise vollständigen Zugriff auf das Netzwerk erlangen.
7. Die Reparatur wird vom Wartungsserver durchgeführt, der Anfälligkeiten und andere Sicherheitsrisiken (die weiter oben erwähnten Complianceregeln) aufspürt und die erforderlichen Patches installiert. Sobald das Gerät repariert ist, wird der Netzwerkzugriffsprozess wiederholt, und das jetzt fehlerfreie (sicherheitskonforme) Gerät erhält Zugriff auf das Unternehmensnetzwerk.

HINWEIS: Compliance-Sicherheitsscans
Das Extra "Sicherheit und Compliance" bietet Ihnen die Möglichkeit, einen auf Compliance ausgerichteten Sicherheitsscan zu erstellen und zu konfigurieren, der Zielgeräte auf Konformität mit benutzerdefinierten Sicherheitsrichtlinien scannt. Ein Compliancescan baut auf dem Inhalt der Compliance-Gruppe auf und kann als geplanter Task oder als Richtlinie ausgeführt werden. Informationen darüber, wie Compliance-

Sicherheitsregeln und -Richtlinien aktualisiert und NAC-Einstellungen neu veröffentlicht werden, finden Sie unter "Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist." auf Seite 572.

Überlegungen zur Netzwerktopologie und zum Design

Wenn Sie LANDesk 802.1X NAC-Unterstützung in einer vorhandenen LANDesk 802.1X-Radius-Serverumgebung implementieren, sollten Sie folgende Probleme nicht außer Acht lassen.

- Der **Wartungsserver** und der **Radius-Server** können auf demselben Rechner installiert werden, wobei sie beim Auftreten von Leistungs- oder Skalierbarkeitsproblemen auf getrennte Serverrechner verschoben werden sollten.
- Der **Netzwerk-Switch** muss für 802.1X-Passthru-Weiterleitung konfiguriert werden.
- Der **Router** muss mit zwei VLAN-Subnetzen konfiguriert werden: das primäre Subnetz ist das Unternehmens-/Produktionsnetzwerk, das sekundäre Subnetz ist das Quarantänenetzwerk (d. h. 802.1X Guest VLAN)
- Das **Quarantänenetzwerk** des Routers sollte Zugriffssteuerungslisten (ACL) verwenden, um den Gerätezugriff ganz auf den Wartungsserver zu beschränken.
- Der **Coreserver** sollte im Quarantänenetzwerk nicht sichtbar sein.

Der folgende Workflow beschreibt den Kommunikationsfluss zwischen den verschiedenen Komponenten in einer 802.1X NAC-Umgebung, wenn auf dem Gerät, mit dem versucht wird, auf das Netzwerk zuzugreifen, der LANDesk 802.1X-Agent installiert ist.

Einrichten eines 802.1X-Radius-Servers oder -Proxys

Wie zuvor bereits erwähnt erweitert LANDesk 802.1X NAC eine bestehende 802.1X NAC-Umgebung durch Funktionen für die Authentifizierung und Compliance. LANDesk 802.1X erfordert einen 802.1X-Radius-Server oder Radius-Proxy.

Wählen Sie eine der folgenden Methoden aus, um LANDesk 802.1X NAC zu implementieren:

- "Verwenden des IAS Radius-Server-Plugins (für MD5)" auf Seite 549
- "Verwenden des Radius-Proxys (für PEAP)" auf Seite 552

HINWEIS: Verwenden Sie das IAS Radius-Server-Plugin, wenn Sie den EAP-Typ MD5 angeben. Verwenden Sie den Radius-Proxy, wenn Sie den EAP-Typ PEAP angeben. (Sie können auch den Radius-Proxy verwenden, wenn Sie über einen Radius-Server verfügen, der kein IAS ist.)

Die nachstehende Abschnitte enthalten Schritt-für-Schritt-Anleitungen für beide Konfigurationen.

WICHTIG: Switch- und Routerkonfiguration
Nach der Einrichtung des Radius-Servers müssen Sie auch Ihren Netzwerk-Switch und -Router für LANDesk 802.1X NAC konfigurieren. Da in jeder Netzwerkumgebung andere Switch- und Router-Hardware verwendet wird, können an dieser Stelle keine spezifische Anweisungen für jeden Hardwaretyp gegeben werden. Befolgen Sie bei der Konfiguration von Switches und Router für 802.1X NAC die bezüglich der Funktions- und Topologieanforderungen gegebenen wesentlichen Hinweise im Thema "802.1X NAC-Komponenten, Prozessablauf und Netzwerktopologie" auf Seite 545. Empfehlungen für Switch- und Routerkonfigurationen und Beispiele für Konfigurationsdateien finden Sie ferner auf der LANDesk Support-Website.

Verwenden des IAS Radius-Server-Plugins (für MD5)

Das 802.1X IAS-Server-Plugin verwenden Sie, wenn Sie für die 802.1X-Authentifizierung einen vorhandenen IAS-Server verwenden oder einen neuen IAS-Server konfigurieren möchten.

In den nachstehenden Schritten erfahren Sie, wie ein IAS-Server installiert (falls erforderlich) und mit dem EAP-Plugin konfiguriert wird. Führen Sie alle Schritte aus, bevor Sie 802.1X NAC in der Konsole aktivieren.

Schritt 1: Installieren Sie den Radius-Server und LTA EAP-Typ

1. Installieren Sie IAS (Internet Authentication Server) auf dem Server, den Sie als Radius-Server für den Remotezugriff einrichten möchten. Sie können IAS von der Windows 2003 CD installieren. (**HINWEIS:** Das Radius-Protokoll wird nur unter Windows 2000 und Windows 2003 unterstützt.) Folgen Sie den Installationsanweisungen.
2. Installieren Sie den LTA EAP-Typ auf dem Radius-Server. LTA EAP ist das proprietäre Authentifizierungsprotokoll. Sie installieren LTA EAP von Ihrem Coreserver. Ordnen Sie dem Coreserver ein Laufwerk zu und führen Sie dann die ausführbare Datei **LTAEAP.EXE** aus, die sich im Verzeichnis \LDMain\Install\Radius befindet.
3. Booten Sie den Server neu, um LTA EAP auf dem Server zu registrieren.

HINWEIS: Sie können diesen neuen EAP-Typ auf der Seite "Remoteserver-Eigenschaften" überprüfen. Navigieren Sie hierfür zu **Systemsteuerung > Verwaltung > Routing und RAS**. Klicken Sie mit der rechten Maustaste auf den Remoteserver, klicken Sie auf **Eigenschaften**, klicken Sie auf die Registerkarte **Sicherheit**, klicken Sie auf **Authentifizierungsmethoden** und klicken Sie dann auf **EAP-Methoden**. Der LTA EAP-Typ sollte in der Liste mit den Methoden zu sehen sein. Wenn LTA EAP nicht in der Liste geführt wird, müssen Sie das Protokoll vom Coreserver installieren.

Schritt 2: Konfigurieren und starten Sie den Remotezugriffsdienst auf dem Radius-Server

1. Klicken Sie auf **Systemsteuerung > Verwaltung > Routing und RAS**.
2. Klicken Sie mit der rechten Maustaste auf den Server und klicken Sie dann auf **Routing und RAS konfigurieren und aktivieren**. Der Setup-Assistenten für den Routing- und RAS-Server wird angezeigt.
3. Klicken Sie auf **Weiter**.
4. Wählen Sie **Benutzerdefinierte Konfiguration** aus und klicken Sie anschließend auf **Weiter**.
5. Wählen Sie **DFÜ-Zugriff** aus und klicken Sie auf **Weiter**.
6. Klicken Sie auf **Fertig stellen**.
7. Beantworten Sie die Eingabeaufforderung mit **Ja**, um den Dienst zu starten.

Schritt 3: Passen Sie den Remote Access Service an (geben Sie EAP als bevorzugte Authentifizierungsmethode für Remotegeräte an)

1. Klicken Sie im Routing und RAS-Tool mit der rechten Maustaste auf den Server, den Sie soeben konfiguriert haben, und klicken Sie auf **Eigenschaften**.
2. Vergewissern Sie sich, dass auf der Registerkarte **Allgemein** die Option **RAS-Server** aktiviert ist.
3. Aktivieren Sie auf der Registerkarte **Sicherheit** das Kontrollkästchen **Extensible-Authentication-Protokoll (EAP)**. (Klicken Sie ggf. auf die Schaltfläche **EAP-Methoden**, um sicherzustellen, dass die neue LTA EAP-Methode in der Liste mit den Methoden angezeigt wird.)

4. Klicken Sie auf **OK**, um das Dialogfeld "Authentifizierungsmethoden" zu schließen.
5. Klicken Sie erneut auf **OK**, um das Dialogfeld "Eigenschaften" zu schließen.

Erstellen einer RAS-Richtlinie (Richtlinie für den Remotezugriff) auf dem Radius-Server

Sie müssen eine RAS-Richtlinie erstellen, die die EAP-Methode zur Authentifizierung verwendet.

Sie können hierfür entweder das IAS- oder das Routing und RAS-Tool verwenden.

Schritt 1: Erstellen Sie die RAS-Richtlinie

1. Klicken Sie unter dem Remoteserver-Knoten mit der rechten Maustaste auf **RAS-Richtlinien** und klicken Sie dann auf **Neu**. Der Assistent für RAS-Richtlinien wird angezeigt.
2. Klicken Sie auf **Weiter**.
3. Wählen Sie als Richtlinientyp **Standard** aus, geben Sie einen Namen für die Richtlinie ein und klicken Sie dann auf **Weiter**. (Hinweis: Geben Sie einen beschreibenden Namen ein, der es einfach macht, die Richtlinie zu identifizieren.)
4. Wählen Sie **Ethernet** als Zugriffsmethode aus und klicken Sie dann auf **Weiter**.
5. Wählen Sie **Benutzer** (nicht Gruppe) für den Zugriff aus und klicken Sie anschließend auf **Weiter**.
6. Wählen Sie als Authentifizierungsmethode **LTA EAP** aus und klicken Sie anschließend auf **Weiter**.
7. Klicken Sie auf **Fertigstellen**, um die RAS-Richtlinie zu erstellen.

Schritt 2: Konfigurieren Sie die RAS-Richtlinie für die Unterstützung von Wired- und Wireless-Netzwerken

1. Klicken Sie mit der rechten Maustaste auf die Richtlinie für den Remotezugriff, die Sie gerade erstellt haben, und klicken Sie dann auf **Eigenschaften**.
2. Aktivieren Sie die Option **RAS-Berechtigung erteilen**, um die Wireless-Unterstützung zu aktivieren.
3. Klicken Sie auf **OK**.

Einrichten (Hinzufügen) von Netzwerk-Switches als Radius-Clients

Als nächstes müssen Sie die mit der 802.1X-Authentifizierung zu verwendenden Netzwerk-Switches (als Radius-Clients) hinzufügen.

Diese Aufgabe wird mit dem IAS-Tool (**IAS > Radius-Clients**) ausgeführt.

Indem Sie einen Switch als Radius-Client hinzufügen, ist der Radius-Server in der Lage, Authentifizierungsanforderungen über diesen Switch zu erkennen und zu verarbeiten.

Erstellen eines allgemeinen Benutzers auf dem Radius-Server.

Sie müssen jetzt einen neuen Benutzer auf dem Radius-Server erstellen, um die Anmeldeinformationen für die Anmeldung zu definieren. Der Benutzername und das Kennwort dieses Benutzers bestimmen die zur Authentifizierung verwendeten Anmeldenachweise für mit 802.1X NAC konfigurierte verwaltete Geräte, die versuchen, auf das Netzwerk zuzugreifen.

Verwenden Sie für diese Aufgabe das Computerverwaltungstool des Servers

So erstellen Sie einen Benutzer auf dem Radius-Server.

1. Klicken Sie auf dem Radius-Server auf **Start > Programme > Verwaltung > Computerverwaltung**.
2. Öffnen Sie **Lokale Benutzer und Gruppen**, klicken Sie mit der rechten Maustaste auf **Benutzer** und klicken Sie dann auf **Neuer Benutzer**.
3. Geben Sie einen Benutzernamen ein.
4. Geben Sie ein Kennwort ein und bestätigen Sie es.
5. Konfigurieren Sie das Kennwort mit folgenden Einstellungen:
   - Deaktivieren Sie das Kontrollkästchen **Benutzer muss das Kennwort ändern**.
   - Aktivieren Sie das Kontrollkästchen **Benutzer kann Kennwort nicht ändern**.
   - Aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab**.
   - Stellen Sie sicher, dass das Kontrollkästchen **Konto ist deaktiviert** deaktiviert ist.
6. Klicken Sie auf **Erstellen**.

Der hier eingegebene Benutzername und das hier eingegebene Kennwort sind die Anmeldeinformationen für die Anmeldung, die der Endbenutzer bereitstellen muss, um erfolgreich auf die Authentifizierungsanforderung während des 802.1X-Authentifizierungsprozesses antworten zu können. Die Anmeldeinformationen werden dann zusammen mit den EAP-Gerätedaten an den Radius-Server weitergeleitet, damit entschieden werden kann, ob das Gerät Zugriff auf das Netzwerk erhält.

Sie können jetzt 802.1X NAC in der Konsole aktivieren. (Das andere Implementierungsverfahren für 802.1X besteht darin, einen Radius-Proxy zu konfigurieren und zu installieren. Weitere Informationen finden Sie unter "Verwenden des Radius-Proxys (für PEAP)" auf Seite 552.)

Aktivieren von LANDesk 802.1X NAC mit dem IAS Radius-Server-Plugin

Nachdem Sie alle oben aufgeführten Setup-Schritte ausgeführt haben, können Sie jetzt LANDesk 802.1X NAC aktivieren.

Diesen Schritt führen Sie von der Konsole aus durch (**Extras > Sicherheit > Network Access Control**).

Damit haben Sie den 802.1X-Authentifizierungsdienst im Wesentlichen auf Ihrem Netzwerk aktiviert. Sie müssen jedoch noch verwaltete Geräte mit dem 802.1X-Agenten konfigurieren, bevor der Netzwerkzugriff verwaltet und über die 802.1X-Authentifizierung durchgesetzt werden kann. Siehe "Bereitstellen des LANDesk 802.1X NAC-Agenten auf verwalteten Geräten" auf Seite 555.

So aktivieren Sie LANDesk 802.1X NAC mit dem IAS Radius-Server-Plugin

1. Klicken Sie mit der rechten Maustaste im Extra **Network Access Control** auf **802.1X** und klicken Sie dann auf **802.1X konfigurieren > Radius-Server**.
2. Aktivieren Sie das Kontrollkästchen **802.1X Radius-Server aktivieren**. Hiermit wird die 802.1X-Authentifizierung (für Geräte mit dem 802.1X-Agenten) in Ihrem Netzwerk unter Verwendung des IAS Radius-Server mit dem von Ihnen konfigurierten EAP-Plugin in Betrieb genommen.
3. Wählen Sie für den **EAP-Typ** "MD5" aus.
4. Wählen Sie **LTA EAP IAS-Plugin verwenden** aus.
5. Klicken Sie auf **Speichern**.

Im nachstehenden Abschnitt wird beschrieben, wie LANDesk 802.1X NAC mithilfe der Radius-Proxy-Methode konfiguriert wird.

Verwenden des Radius-Proxys (für PEAP)

Den Radius-Proxy verwenden Sie, wenn Sie den EAP-Typ PEAP angeben. (Sie können auch den Radius-Proxy verwenden, wenn Sie über einen Radius-Server verfügen, der kein IAS ist.)

Der 802.1X Radius-Proxy kann auf folgenden Radius-Servern installiert werden:

- Cisco ACS
- A10-Netzwerke
- CAMS (Comprehensive Access Management System)
- IAS (Internet Authentication Service)

WICHTIG: Koexistenz mit Radius-Server-Software
Der 802.1X-Radius-Proxy kann mit Servern koexistieren, die Radius-Server-Software ausführen. Wenn Ihr Radius-Server hardwarebasiert ist, sollten Sie den 802.1X-Radius-Proxy auf einem separaten Server installieren.

Der Radius-Proxy verwaltet die Kommunikation zwischen dem Switch und dem Gerät, auf dem der 802.1X-Agent installiert ist. Der Proxy befindet sich in der Mitte: das Gerät authentifiziert sich gegenüber dem Radius-Proxy und der Proxy wiederum leitet die ID und das Kennwort an den Radius-Server weiter. Wenn auf dem Gerät, das den Verbindungsversuch unternimmt, der Agent nicht installiert ist, verweigert der Radius-Proxy den Zugriff.

Aktivieren von LANDesk 802.1X NAC mit dem Radius-Proxy.

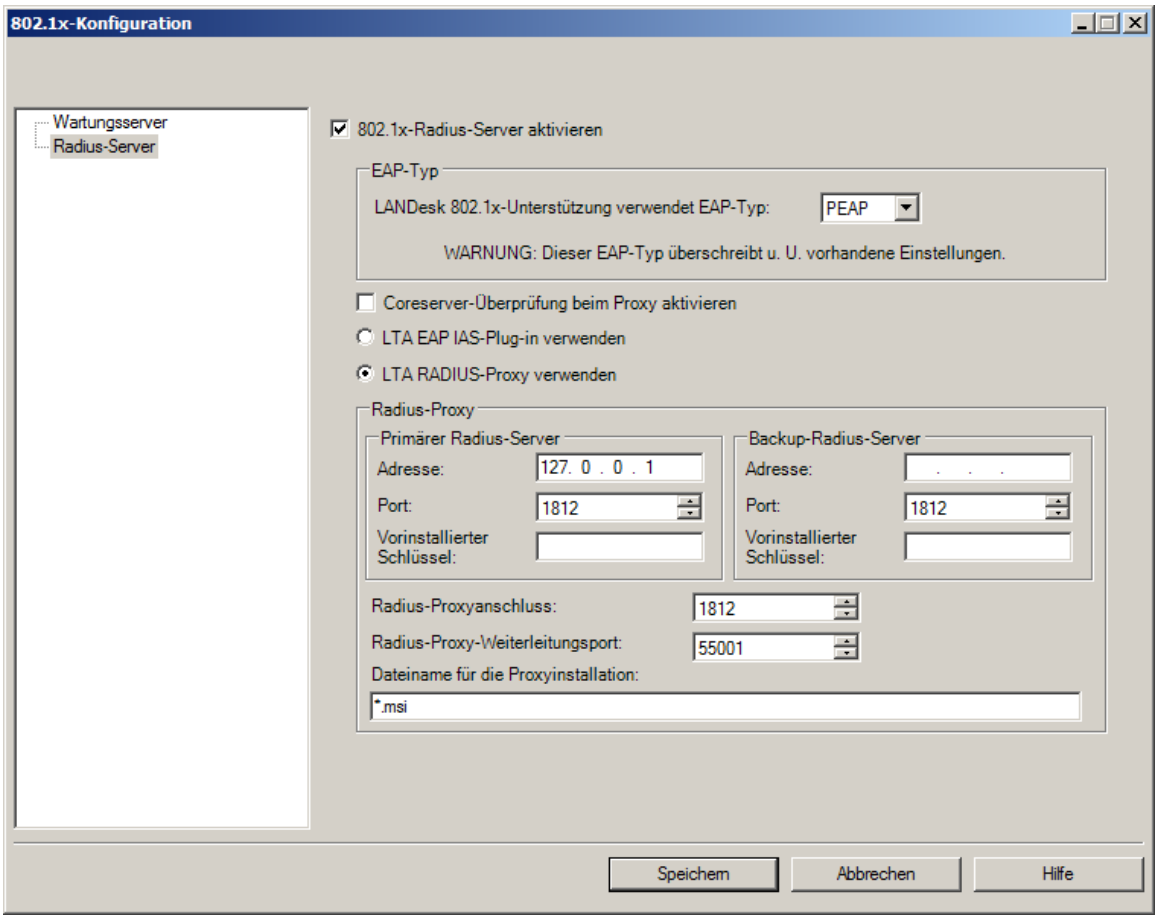
Um den Radius-Proxy verwenden zu können, müssen Sie LANDesk 802.1X NAC aktivieren, die Einstellungen für eine Radius-Proxy-Installationsdatei konfigurieren und den Radius-Proxy auf Ihrem Radius-Server installieren.

Diesen Schritt führen Sie von der Konsole aus durch (**Extras > Sicherheit > Network Access Control**).

Damit haben Sie den 802.1X-Authentifizierungsdienst im Wesentlichen auf Ihrem Netzwerk aktiviert. Sie müssen jedoch noch verwaltete Geräte mit dem 802.1X-Agenten konfigurieren, bevor der Netzwerkzugriff verwaltet und über die 802.1X-Authentifizierung durchgesetzt werden kann. Siehe "Bereitstellen des LANDesk 802.1X NAC-Agenten auf verwalteten Geräten" auf Seite 555.

So aktivieren Sie LANDesk 802.1X NAC und konfigurieren Sie eine Radius-Proxy-Installationsdatei

1. Klicken Sie mit der rechten Maustaste im Extra **Network Access Control** auf **802.1X**, klicken Sie dann auf **802.1X konfigurieren** und schließlich auf **Radius-Server**.



2. Aktivieren Sie das Kontrollkästchen **802.1X Radius-Server aktivieren**. Damit wird die 802.1X-Authentifizierung für Geräte mit dem 802.1X-Agent in Ihrem Netzwerk eingeschaltet (nachdem Sie den Radius-Proxy installiert haben, den Sie hier konfigurieren).
3. Wählen Sie für den **EAP-Typ** "PEAP" aus.
4. Wenn Sie den Coreserver überprüfen wollen, aktivieren Sie das Kontrollkästchen **Coreserver-Überprüfung beim Proxy aktivieren**.
5. Wählen Sie **LTA Radius-Proxy verwenden** aus.
6. Geben Sie die Informationen für einen primären Radius-Server ein. (Wenn Sie einen Backup-Radius-Server verwenden möchten, geben Sie zusätzlich die Informationen für einen sekundären Server ein.)
7. Geben Sie einen Namen für die Radius-Proxy-Installationsdatei (MSI) ein. Die Installationsdatei wird im Verzeichnis LDMAIN\Install\Radius erstellt. Sie können mehrere Radius-Proxy-Installationen einrichten. (**HINWEIS:** Der Radius-Proxy wird auf jeder 32-Bit Windows-Plattform unterstützt.)
8. Klicken Sie auf **Speichern**.

So installieren Sie einen Radius-Proxy

1. Stellen Sie von dem Server aus, den Sie mit dem 802.1X-Radius-Proxy konfigurieren möchten, eine Verbindung mit dem Coreserver her und navigieren Sie zu dem Ordner, in dem Sie die Proxy-Installationsdatei gespeichert haben.
2. Doppelklicken Sie auf die MSI-Datei, um die Installation auszuführen.

3. Klicken Sie auf **Schließen**, wenn die Installation abgeschlossen ist. Ein Neustart des Systems ist nicht erforderlich.

Die Radius-Proxy-Installation fügt Daten in die Serverregistrierung ein (z. B. Adress- und Anschlussdaten).

WARNUNG: 64-Bit-Plattformen werden nicht unterstützt
Installieren Sie den Radius-Proxy *nicht* auf Windows 98 oder auf einer 64-Bit-Plattform.

Im nachstehenden Thema werden die Dialogfelder beschrieben, auf die in den Aufgaben weiter oben Bezug genommen wurde.

Hilfe zu 802.1X und zum Server

Informationen über das Dialogfeld "802.1X-Konfigurationseinstellungen"

Verwenden Sie dieses Dialogfeld, um einen Wartungsserver auszuwählen und die Einstellungen der Netzwerkzugriffsteuerung auf dem Wartungsserver zu veröffentlichen, damit 802.1X NAC auf Ihrem Netzwerk aktiviert wird.

Wenn Sie das IAS Radius-Server-Plugin verwenden, aktivieren Sie ganz einfach den Radius-Server, geben den EAP-Typ an (MD5) und wählen dann die IAS-Plugin-Option aus.

Wenn Sie den Radius-Proxy verwenden, müssen Sie nicht nur den Radius-Server implementieren und den EAP-Typ (PEAP) angeben, sondern darüber hinaus auch eine Radius-Proxy-Installationsdatei konfigurieren und dann den Radius-Proxy auf dem designierten Server installieren.

Dieses Dialogfeld umfasst zwei Registerkarten:

Informationen zur Seite "Wartungsserver"

- **Hinzufügen:** Öffnet ein Dialogfeld, in dem Sie den Wartungsserver angeben können, den Sie zur Reparatur fehlerhafter Geräte im Quarantänenetzwerk verwenden möchten. Weitere Informationen über den Wartungsserver erhalten Sie, wenn Sie auf **Hilfe** klicken. Ein Wartungsserver enthält die Setup- und Supportdateien (Sicherheitsclient, Definitionen für den Sicherheitstyp und erforderliche Patches) sowie HTML-Vorlagenseiten, die beim Scannen von Geräten auf die von Ihrer Sicherheitsrichtlinie bestimmten Anfälligkeiten verwendet werden. Mithilfe dieser Ressourcen repariert der Wartungsserver dann alle erkannten Anfälligkeiten, so dass das Gerät als fehlerfrei oder compliant (konform) gescannt werden kann und daraufhin Netzwerkzugriff erhält.
- **Entfernen:** Löscht den ausgewählten Wartungsserver.
- **Ändern:** Damit können Sie den ausgewählten Wartungsserver bearbeiten.
- **Veröffentlichen:** Öffnet ein Dialogfeld, in dem Sie die NAC-Einstellungen für die Posture-Validierung und für Wartungsserver veröffentlichen.

Informationen zur Seite "Radius-Server"

- **802.1X Radius-Server aktivieren:** Aktiviert die LANDesk 802.1X NAC-Unterstützung (Authentifizierung und Compliance).

  HINWEIS: Diese Option ist standardmäßig deaktiviert; das bedeutet im Wesentlichen, dass jedem Gerät, das eine Verbindung herzustellen versucht, der Zugriff auf das Netzwerk gestattet wird, ganz gleich, ob das Gerät fehlerfrei oder fehlerhaft ist. Lassen Sie diese Option deaktiviert, wenn Sie jedem Gerät Zugriff auf das Netzwerk erteilen möchten.

- **EAP-Typ:** Identifiziert den von der 802.1X-Authentifizierung verwendeten EAP-Typ. Wählen Sie "PEAP" für eine Radius-Proxy-Implementierung aus. Wählen Sie "MD5" für eine IAS Radius-Server-Plugin-Implementierung aus.
- **LTA EAP IAS-Plugin verwenden:** Wählen Sie diese Option, wenn Sie einen vorhandenen IAS-Server verwenden möchten.
- **LTA Radius-Proxy verwenden:** Diese Option verwenden Sie, wenn Sie den EAP-Typ PEAP verwenden wollen. Wenn diese Option ausgewählt wurde, können Sie eine 802.1X Radius-Proxy-Installationsdatei konfigurieren.
- **Radius-Proxy:** Geben Sie die Informationen für einen primären Radius-Server ein. (Wenn Sie einen Backup-Radius-Server verwenden möchten, geben Sie zusätzlich die Informationen für einen sekundären Server ein.)
    - **Radius-Server-Adresse:** Gibt die IP-Adresse Ihres Radius-Servers an.
    - **Radius-Server-Port:** Gibt die Portnummer Ihres Radius-Servers an. Die Standard-Portnummer für die Radius-Authentifizierung ist UDP-Port 1812.
    - **Vorinstallierter Schlüssel:** Gibt den vorinstallierten Schlüssel (bzw. das freigegebene Geheimnis) an, der dafür sorgt, dass die Sicherheit für die Kommunikation zwischen Switch und Radius-Server nicht kompromittiert wird. Der vorinstallierte Schlüssel ist eine Textzeichenfolge. Die Zeichenfolge, die Sie hier eingeben, muss mit der auf dem Switch und auf dem Radius-Server konfigurierten Zeichenfolge des vorinstallierten Schlüssels übereinstimmen.
- **Radius-Proxyanschluss:** Gibt die Anschlussnummer Ihres Radius-Proxy an. Dieser Anschluss kommuniziert mit dem Switch. Beachten Sie, dass die Anschlussnummer sich von der Anschlussnummer des Radius-Servers (s. o.) unterscheiden muss, wenn sie sich auf demselben Computer befinden.
- **Radius-Proxy-Weiterleitungsport:** Gibt die Weiterleitung-Portnummer Ihres Radius-Servers an. Dieser Port leitet Daten an den Radius-Server weiter.
- **Dateiname für die Proxy-Installation:** Identifiziert die Radius-Proxy-Installationsdatei. Die Installationsdatei wird im Verzeichnis LDMain unter Install\Radius\ erstellt. Sie können mehrere Radius-Proxy-Installationsdateien erstellen. Radius-Proxys werden auf jeder 32-Bit Windows-Plattform unterstützt.

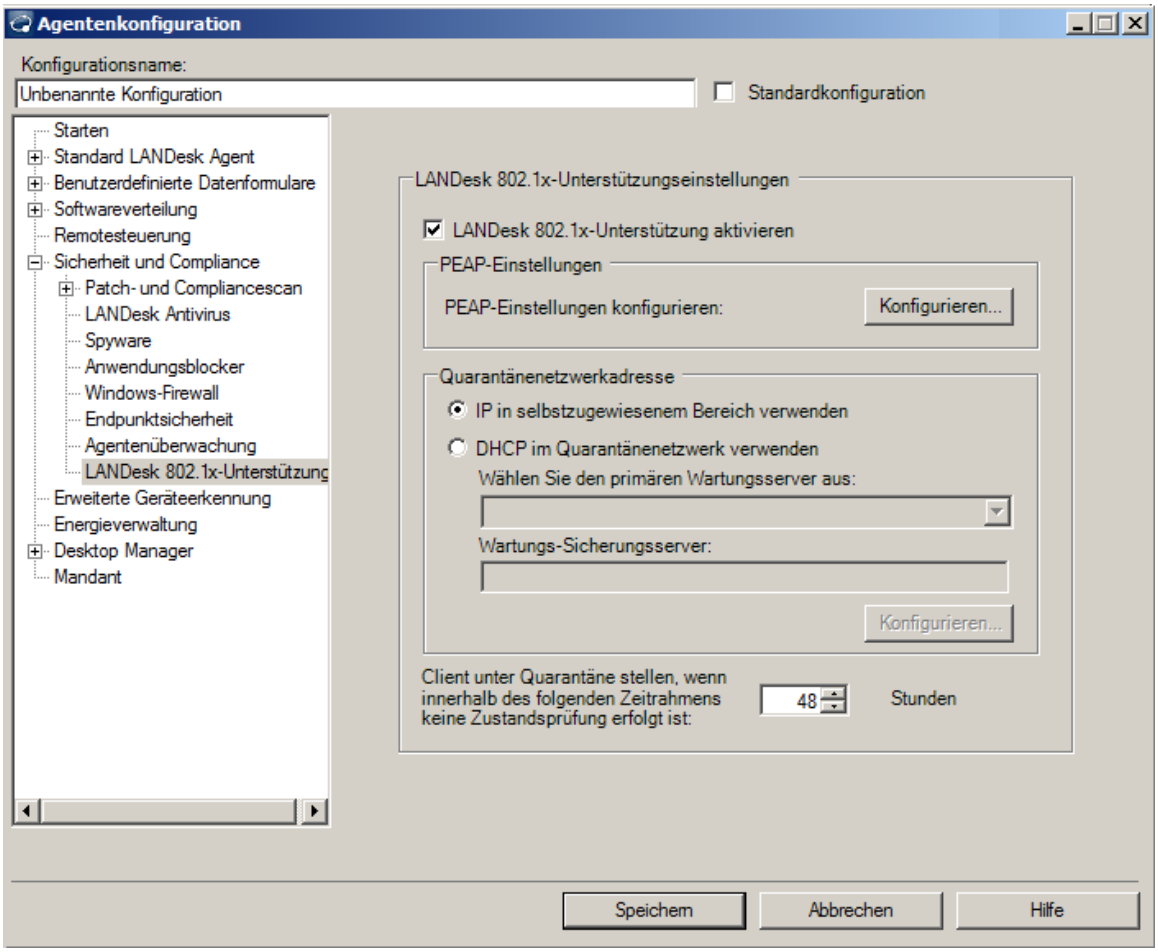
Bereitstellen des LANDesk 802.1X NAC-Agenten auf verwalteten Geräten

Der letzte Schritt beim Einrichten der LANDesk 802.1X NAC-Unterstützung besteht darin, den 802.1X-Agenten auf verwalteten Zielgeräten bereitzustellen.

Auf diese Weise wird der Compliancescan ermöglicht und verwaltete Geräte können authentifiziert werden, damit sie Zugriff aufs Netzwerk erhalten, unter Quarantäne gestellt und repariert werden können.

So stellen Sie den 802.1X-Agenten auf verwalteten Geräten bereit

1. Klicken Sie im Extra **Agentenkonfiguration** auf **Neue Windows-Konfiguration**, öffnen Sie den Knoten **Sicherheit und Compliance** und klicken Sie dann auf **LANDesk 802.1X-Unterstützung**.

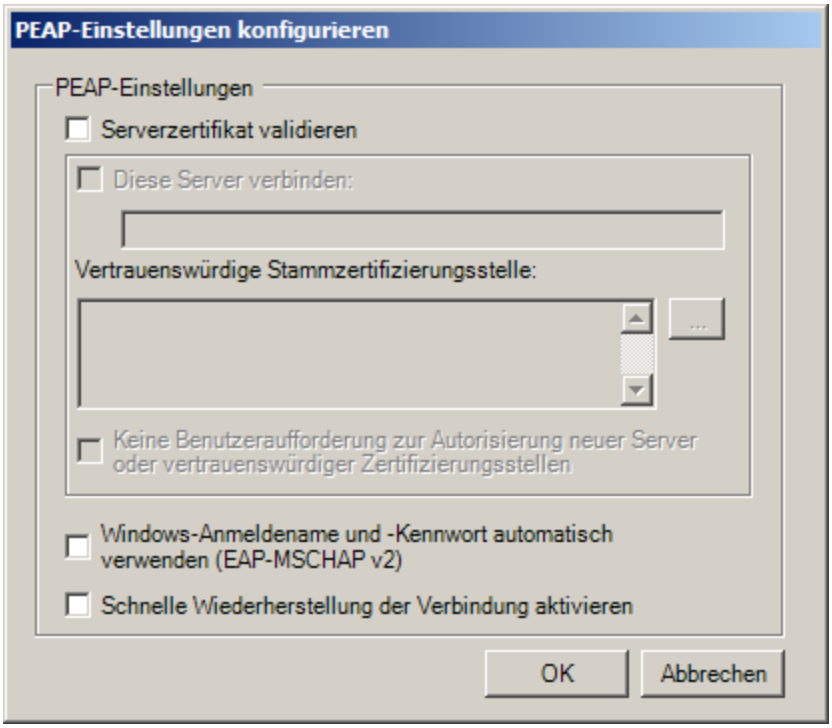


2. Aktivieren Sie das Kontrollkästchen **LANDesk 802.1X-Unterstützung aktivieren**.

   WICHTIG: Diese Option ist nicht verfügbar, wenn Sie den 802.1X Radius-Server nicht bereits im NAC-Tool der Konsole aktiviert haben.

   HINWEIS: 802.1X NAC verwendet den im Extra "NAC" definierten EAP-Typ (PEAP oder MD5). Die Einstellung für den EAP-Typ gilt für den gesamten Core. Mit anderen Worten: Alle mit dieser Agentenkonfiguration konfigurierten Geräte werden mit dem in der Konsole angegebenen EAP-Typ konfiguriert.

3. Wenn Sie den EAP-Typ PEAP verwenden, klicken Sie auf **Konfigurieren**.



4. Definieren Sie die folgenden PEAP-Einstellungen und klicken Sie dann auf **OK**.
   - **Serverzertifikat validieren:** Zeigt an, dass die Zertifikatdatei vom Radius-Server vertrauenswürdig ist.
   - **Diese Server verbinden:** Bietet eine zusätzliche Validierungsmöglichkeit, mit der Sie bestimmte Server definieren, die vertrauenswürdig sind. Geben Sie Servernamen (vollqualifizierte DNS-Namen) durch Leerzeichen getrennt ein.
   - **Vertrauenswürdige Stammzertifizierungsstelle:** Importiert die vertrauenswürdige Zertifikatdatei.
   - **Keine Benutzeraufforderung zur Autorisierung neuer Server:** Schaltet die Benutzeraufforderung zur Autorisierung auf Endbenutzergeräten ab.
   - **Windows-Anmeldename und -Kennwort automatisch verwenden:** Verwendet die Windows-Anmeldeinformationen, so dass diese nicht mehrmals eingegeben werden müssen.
   - **Schnelle Wiederherstellung der Verbindung aktivieren:** Stellt die Anmeldeinformationen in den Cache, damit bei einem Timeout des Geräts eine schnelle Anmeldung möglich ist.
5. Wählen Sie im Dialogfeld "Agentenkonfiguration" die gewünschte Methode aus, mit der als fehlerhaft eingestufte Geräte unter Quarantäne gestellt werden. (Verwenden Sie eine IP-Adresse im selbstzugewiesenen Bereich oder DHCP im Quarantänenetzwerk.)
6. Konfigurieren Sie die automatische Quarantänezeit, indem Sie angeben, wie viele Stunden seit dem letzten Zustandsscan des Geräts vergehen dürfen, bevor es als fehlerhaft gilt und aus dem Unternehmensnetzwerk abgemeldet und unter Quarantäne gestellt wird.
7. Geben Sie ggf. weitere Konfigurationseinstellungen für Geräteagenten an, die Sie für die zu konfigurierenden Zielgeräte übernehmen möchten.

8. Klicken Sie auf **Speichern**.

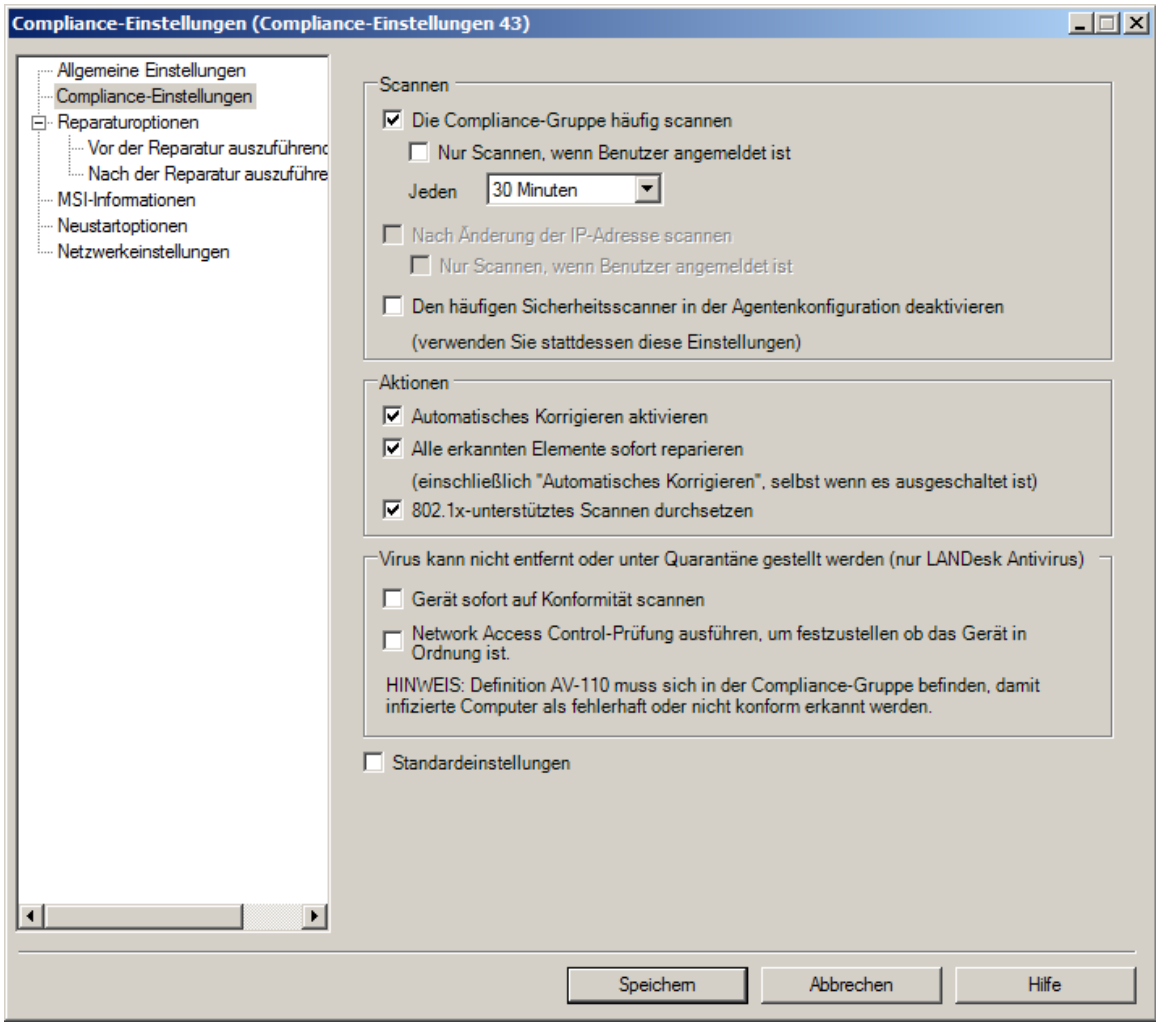
Sie können jetzt die Agentenkonfiguration auf Geräten bereitstellen, die LANDesk 802.1X NAC verwenden sollen, und dann Compliance-Scanaufgaben erstellen, die 802.1X-fähige Geräte auf Compliance mit Ihren Sicherheitsrichtlinien scannen.

Erstellen eines Compliance-Sicherheitsscantasks

Network Access Control (NAC) führt einen Compliance-Sicherheitsscan aus, der die Posture oder den Zustand des Geräts anhand der Kriterien Ihrer benutzerdefinierten Sicherheitsrichtlinie feststellt.

Verwenden von Compliance-Einstellungen

Der Compliancescan wird von einem Compliance-Scantask durchgeführt, der eine Compliance-Einstellung verwendet, bei der die Option **802.1X-unterstütztes Scannen durchsetzen** auf der Registerkarte **Compliance** aktiviert ist.


Compliance-Einstellungen (Compliance-Einstellungen 43)
Allgemeine Einstellungen
Compliance-Einstellungen
Reparaturoptionen
Vor der Reparatur auszuführenc
Nach der Reparatur auszuführe
MSI-Informationen
Neustartoptionen
Netzwerkeinstellungen
Scannen
Die Compliance-Gruppe häufig scannen
Nur Scannen, wenn Benutzer angemeldet ist
Jeden
30 Minuten
Nach Änderung der IP-Adresse scannen
Nur Scannen, wenn Benutzer angemeldet ist
Den häufigen Sicherheitsscanner in der Agentenkonfiguration deaktivieren
(verwenden Sie stattdessen diese Einstellungen)
Aktionen
Automatisches Korrigieren aktivieren
Alle erkannten Elemente sofort reparieren
(einschließlich "Automatisches Korrigieren", selbst wenn es ausgeschaltet ist)
802.1x-unterstütztes Scannen durchsetzen
Virus kann nicht entfernt oder unter Quarantäne gestellt werden (nur LANDesk Antivirus)
Gerät sofort auf Konformität scannen
Network Access Control-Prüfung ausführen, um festzustellen ob das Gerät in Ordnung ist.
HINWEIS: Definition AV-110 muss sich in der Compliance-Gruppe befinden, damit infizierte Computer als fehlerhaft oder nicht konform erkannt werden.
Standardeinstellungen
Speichern
Abbrechen
Hilfe

Zur Erstellung von Compliance-Sicherheitsscans verwenden Sie das Extra "Patch und Compliance" (**Extras > Sicherheit > Patch und Compliance**). Schritt-für-Schritt-Anweisungen finden Sie unter "Erstellen von Tasks für Sicherheits- und Compliancescans" auf Seite 623.

HINWEIS: Compliance-Sicherheitsscans
Das Extra "Sicherheit und Compliance" bietet Ihnen die Möglichkeit, einen auf Compliance ausgerichteten Sicherheitsscan zu erstellen und zu konfigurieren, der Zielgeräte auf Konformität mit benutzerdefinierten Sicherheitsrichtlinien scannt. Ein Compliancescan baut auf dem Inhalt der Compliance-Gruppe auf und kann als geplanter Task oder als Richtlinie ausgeführt werden. Informationen darüber, wie Compliance-Sicherheitsregeln und -Richtlinien aktualisiert und NAC-Einstellungen neu veröffentlicht werden, finden Sie unter "Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist." auf Seite 572.

Konfigurieren eines Switches und eines Routers für LANDesk 802.1X NAC-Unterstützung

LANDesk 802.1X NAC erfordert einen Switch und einen Router zur Durchführung der Authentifizierung und Sicherstellung der Compliance.

Da in jeder Netzwerkumgebung andere Switch- und Router-Hardware verwendet wird, können an dieser Stelle keine spezifische Anweisungen für jeden Hardwaretyp gegeben werden. Befolgen Sie bei der Konfiguration der Switches und Router für LANDesk 802.1X NAC die bezüglich der Funktions- und Topologieanforderungen gegebenen wesentlichen Hinweise in den vorangegangenen Themen. Nähere Informationen finden Sie unter "802.1X NAC-Komponenten, Prozessablauf und Netzwerktopologie" auf Seite 545.

Empfehlungen für bestimmte Switch- und Routerkonfigurationen und Beispiele für Konfigurationsdateien finden Sie ferner auf der LANDesk Support-Website.

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter http://community.landesk.com

Einrichten und Konfigurieren eines Wartungsservers

Network Access Control (NAC) erfordert einen Wartungsserver zur Reparatur anfälliger oder infizierter Geräte. Der Wartungsserver ist die Stelle, an die die Geräte, deren Systemzustand als fehlerhaft ("unhealthy") eingestuft wurde, zur Reparatur gesendet werden, damit sie die Complianceregeln erfüllen können, die Sie für einen fehlerfreien Systemzustand konfiguriert haben.

Der Wartungsserver ist der Server, auf dem Sie Ihre Reparaturressourcen veröffentlichen, beispielsweise die Sicherheitsclients, die Geräte auf Anfälligkeiten und andere Sicherheitsrisiken scannen, Patchdateien und die auf den Geräten eingeblendeten HTML-Seiten, die über Reparaturoptionen oder eingeschränkten Netzwerkzugriff informieren.

Anforderungen für Wartungsserver

Das von Ihnen als Wartungsserver eingerichtete Gerät muss folgende Systemanforderungen erfüllen:

- Als Wartungsserver wird jede Art von Webserver unterstützt, beispielsweise ein IIS-Server unter Windows oder Apache unter Linux.
- Sie müssen eine Webfreigabe auf dem Wartungsserver erstellen, die anonymen Zugriff mit aktivierten Lese- und Navigationsrechten bietet. Ausführliche Anweisungen finden Sie unter "Erstellen einer Webfreigabe auf dem Wartungsserver" auf Seite 560.

WICHTIG: Erstellen Sie eine Samba-Freigabe
Falls Sie einen Apache-Webserver unter Linux verwenden, muss die Freigabe, die Sie erstellen, eine Samba-Freigabe sein.

Bestimmen des Wartungsserverstandorts im Netzwerk

Ihre Entscheidung bzgl. des Standorts des Wartungsservers in Ihrem Netzwerk sollte folgende Richtlinien berücksichtigen.

- Der Wartungsserver kann auf beiden Seiten des Routers installiert werden.
- Wenn Sie den Wartungsserver auf der Clientseite des Routers installieren, bedeutet dies mehr Sicherheit, da Sie keine Ausnahmen für Ihre Routerregeln definieren müssen; jedoch müssen Sie bei dieser Lösung alle Remediation-Dateien manuell auf den Rechner übertragen, sooft Sie die Daten ändern.
- Wenn Sie den Wartungsserver auf der gegenüberliegenden Seite des Routers installieren, gehen Sie ein Sicherheitsrisiko ein, da Quarantänerechner auf einen Rechner in Ihrem Netzwerk zugreifen; jedoch können Sie bei dieser Lösung Remediation-Dateien mithilfe einer Pushprozedur auf den Rechner übertragen, ohne sie manuell dorthin übertragen zu müssen.
- Der Wartungsserver muss vom Remediation-VLAN aus sichtbar sein.
- Sie können mehrere Wartungsserver in Ihrem Netzwerk installieren.

Sie können Diagramme anzeigen, die den Komponentenstandort und den Prozess-Workflow für LANDesk NAC 802.1X im entsprechenden Übersichtsabschnitt veranschaulichen.

Erstellen einer Webfreigabe auf dem Wartungsserver

Der Vorgang der Erstellung und Konfiguration einer Webfreigabe auf dem Reparaturserver wurde für Sie mithilfe eines Skripts automatisiert, das sich auf dem Coreserver befindet. Sie führen das Skript von dem Rechner aus, den Sie als Wartungsserver einrichten möchten.

Die Webfreigabe, die auf dem Wartungsserver erstellt wird, dient als Speicherbereich für die ausführbaren Patchdateien, die zur Reparatur von Anfälligkeiten auf den betroffenen Geräten verwendet werden. Wenn Sie Infrastrukturdateien oder Reparaturquellen vom Coreserver aus veröffentlichen (z. B. Sicherheitsclient, Patchdateien und HTML-Dateien), werden diese Dateien in die Webfreigabe kopiert.

WICHTIG: Die Webfreigabe muss den Namen LDLogon haben
Der Name der Webfreigabe muss LDLogon lauten. Sie können diese Freigabe an einer beliebigen Stelle auf dem Webserver erstellen. Normalerweise sieht der Pfad wie folgt aus: C:\Inetpub\wwwroot\LDLogon. Sie können die Freigabe jedoch an einem beliebigen Standort erstellen, solange die URL-Umleitung auf diesen Pfad konfiguriert wird: http://servername/LDLogon.

Nachdem Sie das Skript zum Erstellen und Konfigurieren der Webfreigabe ausgeführt haben, müssen Sie den Wartungsserver in der Konsole hinzufügen und den Pfad zur Freigabe angeben (ausführliche Anweisungen finden Sie unter "Konfigurieren (Hinzufügen) eines Wartungsservers in der Konsole" auf Seite 561). Dadurch wird sichergestellt, dass der Coreserver Reparaturquellen an der richtigen Stelle auf dem Wartungsserver veröffentlicht.

So führen Sie das Remediation Server-Konfigurationsskript aus

1. Ordnen Sie von dem Rechner aus, den Sie als Wartungsserver einrichten möchten, dem Ordner LDMain\Install\TrustedAccess\RemediationServer Ihres Coreservers ein Laufwerk zu.
2. Doppelklicken Sie auf das CONFIGURE.REMEDIATION.SERVER.VBS-Setupskript.

Automatische Konfiguration des Reparaturservers

Das Remediation Server-Konfigurationsskript konfiguriert den Server automatisch für die Durchführung von Reparaturen durch:

- Erstellen einer Webfreigabe mit dem Namen LDLogon an folgendem Speicherort: c:\inetpub\wwwroot\LDLogon.
- Aktivieren des anonymen Zugriffs auf die LDLogon-Freigabe mit Lese-, Schreib- und Navigationsrechten.
- Hinzufügen eines neuen MIME-Typs für .LRD-Dateien und Festlegen auf application/octet-stream (application/binary).

HINWEIS: Sie können auch das Microsoft IIS-Tool zur manuellen Konfiguration der Zugriffsberechtigungen und MIME-Typen der LDLogon-Freigabe verwenden.

Der Wartungsserver ist nun zur Konfiguration (d. h. zum Hinzufügen) in der Konsole bereit.

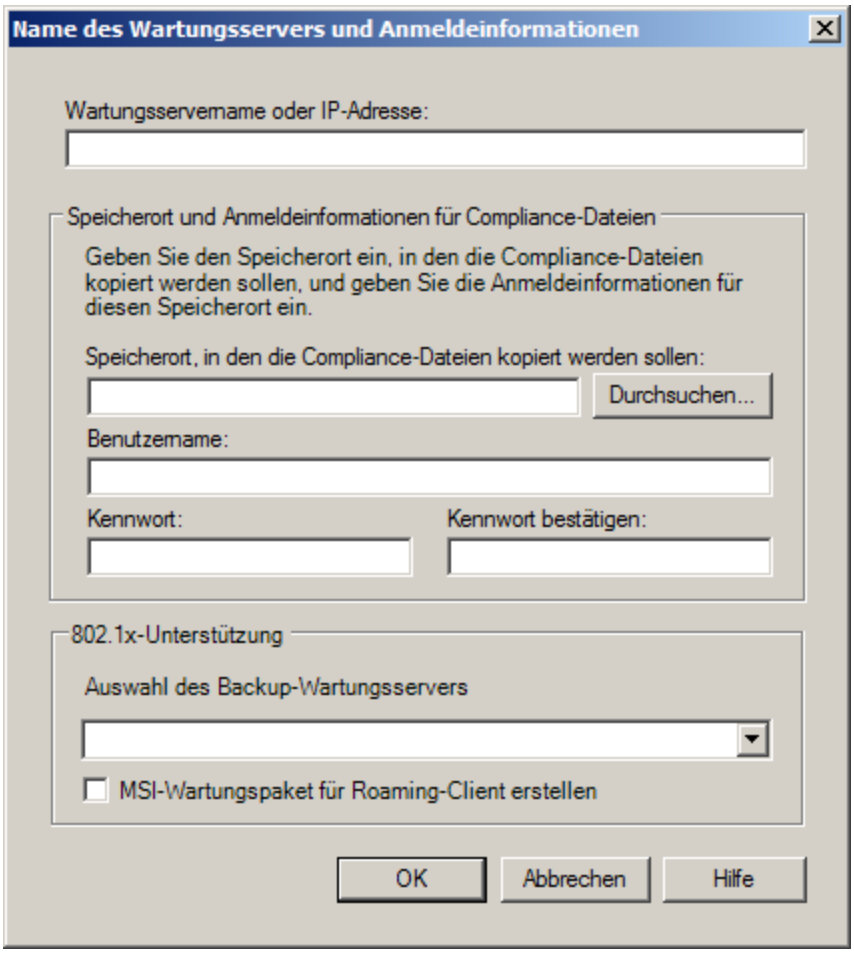
Konfigurieren (Hinzufügen) eines Wartungsservers in der Konsole

Nachdem Sie einen Wartungsserver eingerichtet haben, müssen Sie ihn jetzt der Liste mit den gültigen Wartungsservern im Dialogfeld **Wartungsserver konfigurieren** in der Konsole hinzufügen. Bei diesem Vorgang wird der Wartungsserver im Netzwerk identifiziert und kann von nun an mit den anderen NAC-Komponenten kommunizieren.

So konfigurieren Sie Wartungsserver in der Konsole und fügen sie hinzu

1. Klicken Sie mit der rechten Maustaste im Extra **Network Access Control** auf **802.1X** und klicken Sie dann auf **802.1X konfigurieren**.

2. Klicken Sie auf der Seite **Wartungsserver** auf **Hinzufügen**. Das Dialogfeld **Name des Wartungsservers und Anmeldeinformationen** wird angezeigt.



3. Geben Sie den Servernamen oder die IP-Adresse des Wartungsservers ein.

4. Geben Sie den Pfad zu der Webfreigabe ein (auf dem Webserver, den Sie als Wartungsserver einrichten), in der Sie Compliance-Dateien veröffentlichen möchten. Die Webfreigabe muss LDLogon genannt werden. Compliance-Dateien sind Sicherheitsdefinitionsdateien, die Ihre Compliance-Sicherheitsrichtlinie (d. h. den Inhalt der Gruppe **Compliance** in Patch und Compliance und die zum Reparieren erkannter Anfälligkeiten benötigten Patchdateien) definieren.

   Sie können einen UNC-Pfad oder zugeordneten Laufwerkspfad eingeben. Ein UNC-Pfad ist die zuverlässigste Methode, da Laufwerkszuordnungen sich ggf. ändern (siehe Hinweis weiter unten). Mit der Schaltfläche **Durchsuchen** können Sie zu der Freigabe navigieren, in der Sie auf dem Wartungsserver Compliance-Dateien veröffentlichen möchten.

   Wichtig: Wenn Sie einen lokalen Pfad oder ein zugeordnetes Laufwerk in das Feld **Speicherort, in den die Compliance-Dateien kopiert werden sollen** eingeben, werden die Dateien entweder auf dem lokalen Rechner oder in dem angegebenen zugeordneten Laufwerk des Rechners, auf dem die Veröffentlichung initiiert wird, veröffentlicht. Um zu gewährleisten, dass Compliance-Dateien auf jedem Wartungsserver im Netzwerk im selben Speicherort veröffentlicht werden, wird die Verwendung eines UNC-Pfades, der auf eine Netzwerkfreigabe zeigt, empfohlen.

5. Geben Sie einen gültigen Benutzernamen und ein Kennwort für den Zugriff auf den Wartungsserver ein.
6. Wenn Sie mehr als einen Wartungsserver konfiguriert haben, können Sie einen Backup-Wartungsserver aus der Dropdownliste auswählen.
7. Wenn Sie in der Lage sein wollen, einen Wartungsserver in einem anderen Netzwerk für Geräte zu konfigurieren, die zwischen vertrauenswürdigen Netzwerken verschoben werden, generieren Sie ein Installationspaket (MSI).
8. Klicken Sie auf **OK**, um diesen Wartungsserver zur Liste hinzuzufügen.

Jetzt können Sie die Dateien zur Reparatur der Infrastruktur auf dem Server veröffentlichen (falls Sie auch einen Remediation-Validierungsserver und Benutzeranmeldeinformationen konfiguriert haben).

Informationen zum Dialogfeld "Name des Wartungsservers und Anmeldeinformationen"

Dieses Dialogfeld verwenden Sie, um den Wartungsserver und den Pfad zu der Webfreigabe auf dem Wartungsserver zu bestimmen, in dem die Reparaturquellen (Sicherheitsclients, Patchdateien und HTML-Seiten) veröffentlicht werden.

- **Wartungsservername oder IP-Adresse:** Identifiziert den Wartungsserver anhand seiner IP-Adresse oder eines Hostnamens.
- **Speicherort, in den die Compliance-Dateien kopiert werden sollen:** Gibt den vollständigen Pfad zu der Webfreigabe auf dem Wartungsserver an, in der Compliance-Dateien vom Core veröffentlicht werden. Der Name der Webfreigabe sollte LDLogon lauten. Der Pfad kann entweder ein UNC-Pfad oder ein zugeordneter Laufwerkspfad (oder lokaler Pfad) sein. Ein UNC-Pfad wird empfohlen (lesen Sie hierzu den **wichtigen** Hinweis weiter oben).
- **Durchsuchen:** Öffnet das lokale Windows Explorer-Fenster, in dem Sie zur LDLogon-Freigabe des Wartungsservers navigieren können.
- **Benutzername:** Identifiziert einen gültigen Benutzer mit Anmeldeinformationen für den Zugriff auf die Webfreigabe auf dem Wartungsserver.
- **Kennwort:** Identifiziert das Kennwort des Benutzers.
- **Kennwort bestätigen:** Bestätigt das Kennwort des Benutzers.

- **OK:** Speichert die Wartungsserver-Einstellungen und fügt sie der Liste im Dialogfeld "Wartungsserver konfigurieren" hinzu.
- **Auswahl des Backup-Wartungsservers:** Wenn Sie mehr als einen Wartungsserver konfiguriert haben, können Sie einen Backup-Wartungsserver aus der Dropdownliste auswählen.
- **MSI-Wartungspaket für Roaming-Client erstellen:** Diese Option verwenden Sie für die Erstellung eines Installationspakets (MSI), das Sie zur Konfiguration eines Wartungsservers in einem anderen Netzwerk verwenden, und zwar für portable Geräte, die in andere vertrauenswürdige Netzwerke verschoben werden.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Einstellungen zu speichern und ohne einen Eintrag zur Liste mit den Wartungsservern hinzuzufügen.

Veröffentlichen von Dateien zur Reparatur der Infrastruktur auf Wartungsservern

Der nächste Schritt beim Einrichten und Konfigurieren eines Wartungsservers ist die Veröffentlichung vitaler Infrastruktur-Reparaturressourcen des Coreservers auf dem Wartungsserver. Zu diesen Infrastruktur-Reparaturressourcen gehören:

- Sicherheitsclient (Dienstprogramm zum Scannen nach Anfälligkeiten)
- Patches, die zu den Anfälligkeiten in der Compliance-Gruppe gehören
- HTML-Seiten, die Verknüpfungen bereitstellen, die Endbenutzern Folgendes ermöglichen: Installieren von Trust-Agenten, Durchführen von Compliance-Sicherheitsscans sowie Reparieren erkannter Anfälligkeiten und anderer Probleme.

Vor dem Veröffentlichen auf Servern müssen Sie zunächst Ihre Compliance-Sicherheitskriterien im Extra "Patch und Compliance" definieren.

Weitere Informationen zu diesen Tasks finden Sie unter "Definieren von Compliance-Sicherheitskriterien im Extra "Patch und Compliance"" auf Seite 564.

Definieren von Compliance-Sicherheitskriterien im Extra "Patch und Compliance"

Nachdem Sie die LANDesk 802.1X NAC-Unterstützung in Ihrer Umgebung eingerichtet haben, können Sie diese Sicherheitsverwaltungstasks im Compliance-Umfeld durchführen.

HINWEIS: Für LANDesk 802.1X NAC sind zusätzliche Server erforderlich
Sie sollten für Ihre Network Access Control (NAC)-Lösung bereits einen Wartungsserver eingerichtet und in der Konsole konfiguriert (oder hinzugefügt) haben. 802.1X erfordert ferner einen 802.1X-Radius-Server. Nähere Informationen finden Sie unter "Einrichten und Konfigurieren eines Wartungsservers" auf Seite 559 bzw. unter "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543.

Weitere Sicherheitsverwaltungsaufgaben im Compliance-Umfeld

Wenn Sie mehr über das Compliance-Scanning und andere NAC-Verwaltungsaufgaben wie das Aktualisieren von Compliance-Sicherheitsregeln und -Richtlinien auf Posture Validation-Servern, das Aktualisieren von Reparaturressourcen auf Wartungsservern, das Hinzufügen von nicht verwalteten Geräten zum Tool "Erkennung nicht verwalteter Geräte", das Anzeigen betroffener Geräte sowie das Konfigurieren der Protokollfunktion und Generieren von Berichten erfahren möchten, lesen Sie die Ausführungen unter "Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist." auf Seite 572.

Definieren von Compliance-Sicherheitskriterien

Die Kriterien für die Compliance-Sicherheit werden von den folgenden Faktoren bestimmt:

- dem Sicherheitsinhalt in der **Compliance-Gruppe** im Extra "Patch und Compliance" und
- der **automatischen Quarantänezeiteinstellung**, die Sie in der Agentenkonfiguration auf der Seite **LANDesk 802.1X-Unterstützung** definiert haben.

Im Folgenden werden die entsprechenden Vorgehensweisen für jede dieser Aufgaben aufgeführt. Siehe "Das Extra "LANDesk 802.1X NAC" – Übersicht" auf Seite 543.

Informationen über Abonnements für Sicherheitsinhalte

Sie müssen im Besitz eines LANDesk Security Suite Inhaltsabonnements sein, um die verschiedenen Sicherheitsinhaltstypen, z. B. Anwendungs- und Betriebssystem-Anfälligkeitsdefinitionen (und die erforderlichen Patches), Spyware-Definitionen, Definitionen für blockierte Anwendungen, Virendefinitionen, Definitionen für Systemkonfigurations-Sicherheitsbedrohungen usw. downloaden zu können.

Ohne eine Security Suite Lizenz können Sie nicht auf die Security-Dienste zugreifen und auch keine Compliance-Sicherheit unter Verwendung dieser Sicherheitsdefinitionen definieren.

Download von Sicherheitstypdefinitionen

Verwenden Sie das Extra "Patch und Compliance" zum Downloaden unterschiedlicher Sicherheitstypdefinitionen, beispielsweise Anfälligkeiten, Spyware und Definitionen für Sicherheitsbedrohungen. Weitere Informationen zur Verwendung der Downloadfunktionen von Patch und Compliance finden Sie unter "Download von Updates für Sicherheitsinhalte" auf Seite 600.

Verwenden der Compliance-Gruppe zum Definieren einer Compliance-Sicherheitsrichtlinie

Wie weiter oben erläutert, ist der Inhalt der Gruppe "Compliance" Ihre Baseline für die Compliance-Sicherheitsrichtlinie. Sie haben die Möglichkeit, entweder nur eine minimale Compliance-Sicherheit zu definieren, die nur eine geringe Anzahl von Definitionen für Anfälligkeiten und Sicherheitsbedrohungen beinhaltet, oder Sie können eine komplexe, strenge Richtlinie erstellen, die mehrere Sicherheitsdefinitionen einschließt. Sie können die Compliance-Sicherheitsrichtlinie außerdem jederzeit bearbeiten, indem Sie einfach nur Definitionen aus der Gruppe "Compliance" hinzufügen bzw. entfernen.

HINWEIS: Erforderliches "Patch und Compliance"-Recht
Nur ein Administrator oder ein Benutzer, der über das Recht "Patch und Compliance" verfügt, kann Definitionen zur Gruppe "Compliance" hinzufügen oder daraus entfernen.

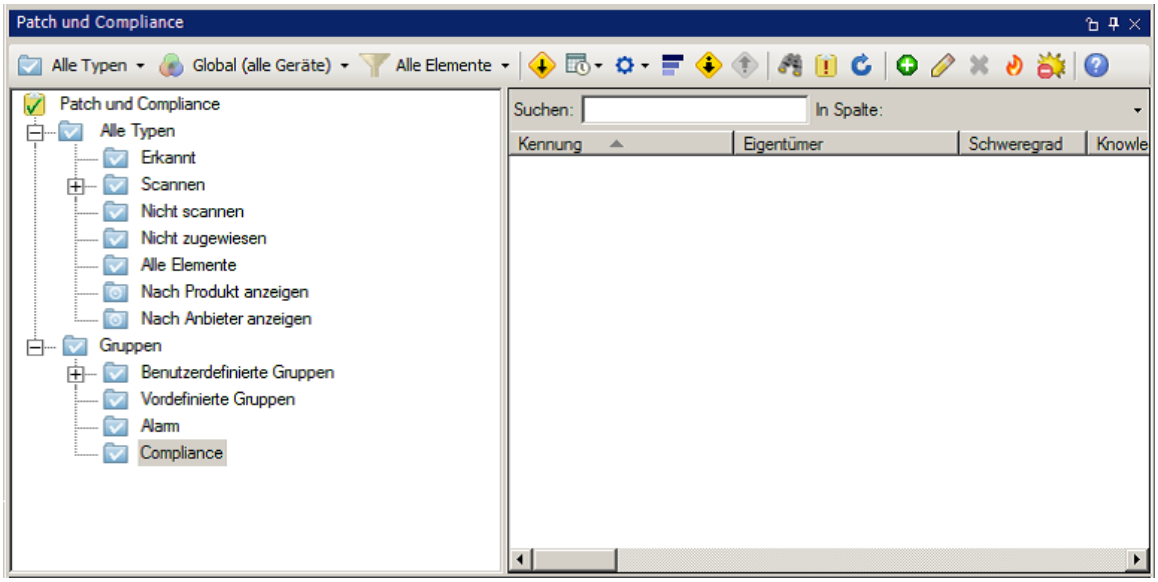
Die folgenden Sicherheitsinhaltstypen können der Gruppe "Compliance" hinzugefügt werden, um eine Compliance-Sicherheitsrichtlinie zu definieren:

- Virenschutzdefinitionen
- Benutzerdefinierte Definitionen
- Definitionen für Treiberupdates
- Definitionen für LANDesk Softwareupdates
- Definitionen für Sicherheitsbedrohungen (einschließlich Firewall-Definitionen)
- Definitionen für Softwareupdates
- Spyware-Definitionen
- Anfälligkeitsdefinitionen (Betriebssystem und Anwendung)

HINWEIS: Das Hinzufügen von Definitionen für blockierte Anwendungen zur Gruppe "Compliance" wird beim Definieren von Compliance-Sicherheitsrichtlinien nicht unterstützt.

So fügen Sie der Compliance-Gruppe Sicherheitsdefinitionen hinzu

1. Wählen Sie im Extra **Patch und Compliance** in der Dropdownliste **Typ** die Art des Sicherheitsinhalts aus, den Sie zu Ihrer Compliance-Sicherheitsrichtlinie hinzufügen möchten, und ziehen Sie dann die entsprechenden Definitionen aus der Elementliste auf die Gruppe **Compliance** und legen Sie sie dort ab.



2. Sie können auch mit der rechten Maustaste auf eine einzelne Definition oder eine ausgewählte Gruppe von Definitionen klicken und dann auf **Zur Compliance-Gruppe hinzufügen** klicken.
3. Vergewissern Sie sich, dass die nötigen zugehörigen Patches gedownloadet werden, bevor Sie den NAC-Inhalt auf Posture Validation-Servern und Wartungsservern veröffentlichen. Sie können mit der rechten Maustaste auf eine Definition, eine ausgewählte Gruppe von Definitionen oder auf die eigentliche **Compliance**-Gruppe und dann auf **Verknüpfte Patches downloaden** klicken, um die zur Reparatur der betroffenen Geräte benötigten Patches downzuloaden.

Veröffentlichen von NAC-Einstellungen für Server

Beim Veröffentlichen von NAC-Einstellungen werden Informationen und Ressourcen an Posture Validation- und Wartungsserver gesandt, die zur Implementierung des Posture-Validierungsvorgangs und zur Durchsetzung der Compliance-Sicherheit erforderlich sind.

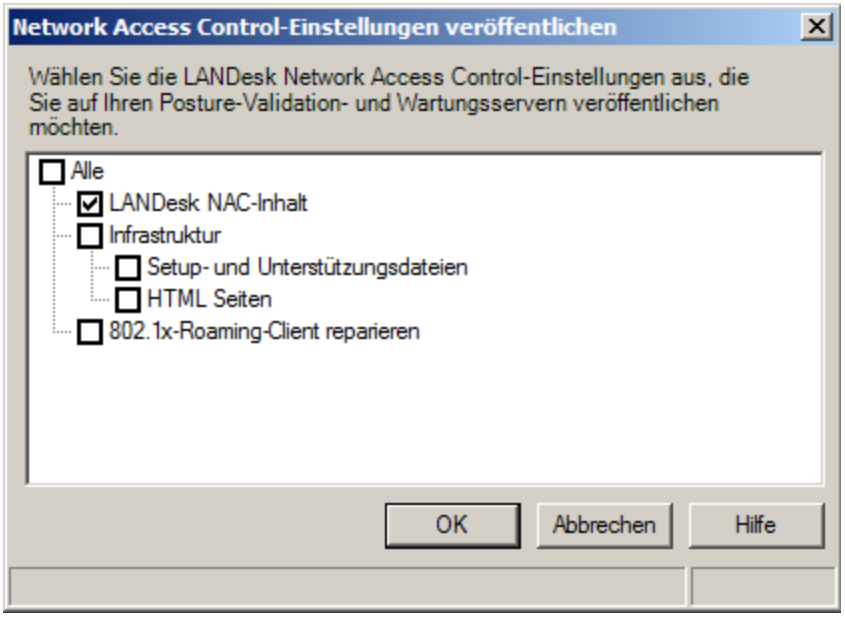
Um NAC-Einstellungen von der Konsole aus zu veröffentlichen, müssen Sie mindestens einen Wartungsserver und die Anmeldeinformationen des Benutzers konfigurieren.

HINWEIS: Die erstmalige Veröffentlichung muss ALLE Einstellungen einschließen
Bei der erstmaligen Veröffentlichung der NAC-Einstellungen auf Ihren Posture Validation- und

Wartungsservern müssen Sie *alle* NAC-Einstellungen einschließen, auch die NAC-Inhalts- und Infrastrukturdateien. (Einzelheiten zu diesen Dateien finden Sie im Folgenden.) Nachfolgende Veröffentlichungen können entweder NAC-Inhalt oder nur Compliance-Regeln enthalten. Im Normalfall müssen die Infrastrukturdateien nur einmal auf den Wartungsservern veröffentlicht werden.

So veröffentlichen Sie die NAC-Einstellungen

1. Im Extra "Network Access Control" können Sie von mehreren Stellen aus auf das Dialogfeld **NAC-Einstellungen veröffentlichen** zugreifen. Sie können beispielsweise mit der rechten Maustaste auf das Objekt **Network Access Control** oder die **Compliance**-Gruppe und dann auf **Veröffentlichen** klicken. Sie können auch die Schaltfläche **Veröffentlichen** in den Dialogfeldern **NAC konfigurieren** und **Wartungsserver konfigurieren** verwenden. Darüber hinaus können Sie auch auf die Symbolleistenschaltfläche **NAC-Einstellungen veröffentlichen** klicken.



2. Um alle NAC-Einstellungen, einschließlich der NAC-Inhalts- und Infrastrukturdateien, in einem Vorgang auf allen Posture Validation- und Wartungsservern zu veröffentlichen, aktivieren Sie das Kontrollkästchen **Alle** und klicken Sie dann auf **OK**.
3. Falls Sie nur den NAC-Inhalt (Sicherheitsdefinitionen, NAC-Einstellungen oder Compliance-Regeln sowie zugehörige Patches) auf Posture Validation- und Wartungsservern veröffentlichen möchten, aktivieren Sie das Kontrollkästchen **NAC-Inhalt** und klicken Sie dann auf **OK**.
4. Wenn Sie nur die Infrastrukturdateien (Sicherheitsclientscanner, Trust-Agent-Installationen und HTML-Seiten) auf Wartungsservern veröffentlichen möchten, aktivieren Sie das Kontrollkästchen **Infrastruktur** und klicken Sie dann auf **OK**. (Im Normalfall müssen Sie die Infrastrukturdateien nur einmal auf den Wartungsservern veröffentlichen.)

Informationen zum Dialogfeld "NAC-Einstellungen veröffentlichen"

Dieses Dialogfeld verwenden Sie zum Veröffentlichen von NAC-Einstellungen auf Posture Validation-Servern und zum Veröffentlichen von Reparatureinstellungen (Ressourcen) auf Wartungsservern in Ihrem Netzwerk.

- **Alle:** Veröffentlicht sowohl NAC-Inhalts- als auch Infrastrukturdateien auf den entsprechenden Servern.
- **NAC-Inhalt:** Veröffentlicht den NAC-Inhalt und die im Extra "Patch und Compliance" definierten Einstellungen auf allen Posture Validation- und Wartungsservern, die zu Ihrem Netzwerk hinzugefügt wurden.
  Wichtig: Sie müssen mindestens über einen Posture Validation-Server in Ihrem Netzwerk verfügen, um den NAC-Inhalt zu veröffentlichen.
  Der NAC-Inhalt repräsentiert die Anfälligkeits- und andere Sicherheitsinhaltstyp-Definitionen, die sich zur Zeit in der Gruppe **Compliance** im Extra "Patch und Compliance" befinden, und er repräsentiert die NAC-Einstellungen (z. B. Einstellungen für fehlerfreie und fehlerhafte Postures, Protokolliergrad usw.), die im Dialogfeld **NAC-Einstellungen konfigurieren** definiert sind. Sicherheitsdefinitionen, Einstellungen für fehlerfreie und fehlerhafte Postures und Protokolliergrad werden auf Posture Validation-Servern veröffentlicht, während zugehörige Patchdateien auf Wartungsservern veröffentlicht werden (basierend auf dem Inhalt der Compliance-Gruppe zum Zeitpunkt der Veröffentlichung).
  (**HINWEIS:** Falls Sie den Inhalt der Gruppe **Compliance** oder NAC-Einstellungen im Dialogfeld **NAC konfigurieren** ändern, müssen Sie diese Daten erneut auf Ihren Servern veröffentlichen.)
- **Infrastruktur:** Veröffentlicht die folgenden Reparaturressourcen auf allen Wartungsservern, die Ihrem Netzwerk hinzugefügt wurden.
  - **Setup und Unterstützungsdateien:** Setup- und Unterstützungsdateien repräsentieren den Sicherheitsclientscanner und die Trust-Agent-Installationen. Der Sicherheitsclientscanner führt Sicherheitsscans und Reparaturen auf Geräten aus.
  - **HTML-Seiten:** Repräsentiert die HTML-Vorlagenseiten, die vom Wartungsserver Geräten zur Verfügung gestellt werden, auf denen Trust-Agenten installiert sind, und die versuchen, auf Ihr Unternehmensnetzwerk zuzugreifen. Diese Seiten informieren den Endanwender, wie er vorgehen muss, um eingeschränkten Zugriff auf das Netzwerk zu erhalten, oder wie er seine Computer reparieren kann, damit sie Konformität mit Ihren Sicherheitsrichtlinien erlangen und vollständigen Zugriff auf das Unternehmensnetzwerk erhalten. Diese HTML-Seiten sind Vorlagen, die Sie modifizieren können. (**HINWEIS:** Im Normalfall müssen Infrastrukturdateien nur einmal auf den Wartungsservern veröffentlicht werden. Im Gegensatz zum NAC-Inhalt (Compliance-Kriterien) müssen Sie diese Dateien nicht bei jeder Änderung der Compliance-Sicherheitsrichtlinie neu veröffentlichen.)

Verwenden der vordefinierten Reparaturseiten

Die NAC-Wartungsseiten sind HTML-Dateien, die mithilfe des Extras "NAC-Einstellungen veröffentlichen" auf der Konsole auf den Wartungsservern veröffentlicht werden. Diese Wartungsseiten sind Teil der Reparatur-Infrastrukturdateien. Im Normalfall müssen diese Dateien nur einmal auf den Wartungsservern veröffentlicht werden.

Die HTML-Dateien werden in dem folgenden Ordner auf dem Coreserver gespeichert:

ManagementSuite\Install\TrustedAccess\RemediationServer

Bei den HTML-Seiten handelt es sich lediglich um Vorlagen, die Sie nach Bedarf an Ihre eigenen Compliance-Sicherheitsbedingungen und -Anforderungen anpassen können. Wenn Sie weitere Informationen dazu erhalten möchten, wie die HTML-Seiten angepasst werden, lesen Sie die Ausführungen unter "Anpassen der Reparaturseiten" auf Seite 570.

Die nachstehenden Abschnitte beschreiben den Zweck der einzelnen HTML-Seiten.

Seite für den Status "Fehlerfrei" ("healthy")

Diese HTML-Seite informiert den Endbenutzer eines Verbindungsgeräts, dass die Posture (der Status) des Geräts überprüft und in Übereinstimmung mit den Compliance-Sicherheitsvorschriften als fehlerfrei bewertet wurde und das Gerät Zugriff auf das Unternehmensnetzwerk erhalten hat.

Der Name dieser HTML-Seite ist: Healthy.html

Die Seite "fehlerfreier Status" wird *nur* angezeigt, wenn der Zustand eines Geräts sich von fehlerhaft in fehlerfrei ändert. Sie wird nicht jedes Mal angezeigt, wenn ein Gerät als fehlerfrei ausgewiesen wird.

Der URL zu dieser Seite auf dem Wartungsserver sollte von Ihnen bei der Konfiguration des Wartungsservers in das Feld **Fehlerfreier URL** eingegeben werden.

Statusseite für Erstbesucher:

Diese HTML-Seite informiert Besucher Ihres Unternehmensnetzwerks, dass Ihr Netzwerk mit Compliance- oder Network Access Control-Sicherheitseinstellungen konfiguriert ist und Benutzer entweder im Web surfen (nur Internetzugriff) oder ihren Computer auf Anfälligkeiten oder andere Sicherheitsrisiken untersuchen (und etwaige Risiken beseitigen) lassen können, bevor der Zugriff auf das Unternehmensnetzwerk gewährt wird. Diese HTML-Seite stellt Verknüpfungen bereit, die entweder nur Zugriff auf das Internet gewähren oder dem Besucher die Möglichkeit bieten, die erforderliche Software für Compliance-Scanning und Reparaturvorgänge herunterzuladen, damit dem Gerät des Besuchers Zugriff auf das Netzwerk erteilt werden kann.

Der Name dieser Seite ist: Visitor.html

Diese Seite enthält Links, die dem Benutzer entweder nur Internetzugriff erteilen oder ihm die Möglichkeit geben, den Trust-Agenten und die Wartungssoftware herunterzuladen und zu installieren, die erforderlich ist, um das Gerät zu reparieren, zu scannen und vollständig auf das Netzwerk zugreifen zu lassen.

Der URL zu dieser Seite auf dem Wartungsserver sollte von Ihnen bei der Konfiguration des Wartungsservers in das Feld **URL für Erstbesucher** eingegeben werden.

Seite für den Mitarbeiterstatus "Fehlerhaft" (Unhealthy")

Diese HTML-Seite informiert den Endbenutzer des Verbindungsgeräts, dass sein Gerät gescannt und festgestellt wurde, dass dieses gegen mindestens eine Vorschrift der Compliance-Sicherheit verstößt, dass das Gerät deshalb als fehlerhaft eingestuft und der Zugriff auf das Netzwerk verweigert wird. Der Netzwerkadministrator sollte diese HTML-Seite so anpassen, dass für den Benutzer ersichtlich wird, welche Anfälligkeiten oder anderen Sicherheitslücken auf dem Gerät erkannt wurden; darüber hinaus sollte diese Seite genaue Instruktionen zur Beseitigung dieser Risiken enthalten. Nachdem das Gerät repariert wurde, muss sich der Endbenutzer erneut beim Netzwerk anmelden, um Zugriff zu erhalten.

Der Name dieser Seite ist: FailedEmployee.html

Der URL zu dieser Seite auf dem Wartungsserver sollte von Ihnen bei der Konfiguration des Wartungsservers in das Feld **URL für Mitarbeiter nach fehlgeschlagenem Verbindungsversuch** eingegeben werden.

Seite für den Besucherstatus "Fehlerhaft" (Unhealthy")

Diese Seite informiert Besucher Ihres Unternehmensnetzwerks, dass ihr Gerät gescannt wurde und gegen mindestens eine Vorschrift der Compliance-Sicherheit verstößt und deshalb keinen Zugriff auf das Netzwerk erhält. Wie die Seite "Unhealthy employee status" (Mitarbeiterstatus "fehlerhaft") können Netzwerkadministrator diese HTML-Seite so anpassen, dass ersichtlich wird, welche Anfälligkeiten oder anderen Sicherheitslücken auf dem Gerät erkannt wurden; darüber hinaus sollte diese Seite genaue Instruktionen zur Beseitigung dieser Risiken enthalten. Sobald das Gerät repariert ist, sollte der Besucher auf das Symbol "Sicherheitsscan für Netzwerkzugriff" klicken, das jetzt auf seinem Desktop zu sehen sein sollte.

Der Name dieser Seite ist: FailedVisitor.html

Der URL zu dieser Seite auf dem Wartungsserver sollte von Ihnen bei der Konfiguration des Wartungsservers in das Feld **URL für Besucher nach fehlgeschlagenem Verbindungsversuch** eingegeben werden.

Anpassen der Reparaturseiten

Wie weiter oben erwähnt, handelt es sich bei den HTML-Reparaturseiten lediglich um Vorlagen, die von Ihnen manuell bearbeitet und geändert werden können, um sie auf Ihre spezifischen Compliance-Sicherheitsanforderungen und -Richtlinien abzustimmen.

Sie können die HTML-Dateien mit jedem beliebigen HTML-Editor bearbeiten. Sie können den vorhandenen Text ändern, um zusätzliche Informationen bereitzustellen, die sich konkret auf Ihr Unternehmensnetzwerk beziehen, und Sie können HTML DIV-Abschnitte für die Sicherheitsdefinitionen hinzufügen, die in Ihrer Compliance-Sicherheitsregel eingeschlossen sind (d. h. die in der Gruppe **Compliance** im Extra "Patch und Compliance" enthaltenen Definitionen).

Beachten Sie, wenn Sie eine HTML-Datei auf dem Coreserver ändern, nachdem sie auf Wartungsservern veröffentlicht wurde, dass Sie die Dateien erneut auf den Wartungsservern veröffentlichen müssen, damit sie Verbindungsgeräten präsentiert werden können (wählen Sie im Dialogfeld **NAC-Einstellungen veröffentlichen** unter der Gruppe **InfrastrukturHTML-Seiten** aus).

Hinzufügen von DIV-Abschnitten, um Sicherheitsdefinitionen, deren Reparatur misslungen ist, dynamisch anzuzeigen

Es kann sich als besonders nützlich für Endanwender und Besucher Ihres Netzwerks erweisen, wenn Sie die "fehlgeschlagenen" (oder fehlerhaften) Seiten so anpassen, dass für Benutzer und Besucher erkennbar wird, welche Sicherheitsprobleme ihre Computer aufweisen und wie sie sich beheben lassen, damit das Gerät erneut gescannt und als fehlerfrei bewertet sowie vollständigen Zugriff auf das Netzwerk erhalten kann.

Diese Seiten sind so ausgelegt, dass Inhalt dynamisch angezeigt wird, wenn eine erkannte Anfälligkeit vom Remediation-Tool des Sicherheitsscanners nicht repariert werden kann. Mit anderen Worten: Wenn das Endbenutzergerät gescannt wird und Anfälligkeiten oder andere Sicherheitslücken erkannt werden (z. B. Systemkonfigurations-Sicherheitsbedrohungen, Spyware etc.) und der Reparaturauftrag fehlschlägt, kann die HTML-Seite "fehlgeschlagen" (oder "fehlerhaft") diese spezifischen Sicherheitsdefinitionen (identifiziert anhand ihrer eindeutigen ID) zusammen mit anderen Informationen anzeigen, die dem Endbenutzer mitteilen, wie sich das Problem beheben lässt; Voraussetzung hierfür ist, dass der Systemadministrator einen DIV-Abschnitt für diese Sicherheitsdefinition hinzugefügt hat (siehe DIV-Beispielabschnitt weiter unten). Wenn der Versuch, eine Sicherheitsdefinition zu reparieren, fehlschlägt und die betreffende Definition nicht über einen DIV-Abschnitt in der HTML-Datei verfügt, werden keine Informationen, die sich speziell auf diese Definition beziehen, im Browser des Endbenutzergeräts angezeigt.

So passen Sie eine HTML-Seite an

1. Öffnen Sie die HTML-Datei in Ihrem HTML-Editor.
2. Bearbeiten Sie einen der vorhandenen Textbausteine, um die Detailinformationen bereitzustellen, die auf dem Bildschirm Ihrer Endbenutzer (Mitarbeiter und Besucher des Unternehmens) angezeigt werden sollen, wenn diese sich bei Ihrem Unternehmensnetzwerk anmelden.
3. Gehen Sie für "fehlgeschlagene HTML-Seiten" wie folgt vor: Fügen Sie für die Sicherheitsinhaltsdefinitionen, die Sie in der Compliance-Gruppe hinterlegt haben, die Ihre Compliance-Sicherheitsrichtlinie definiert, neue DIV-Abschnitte in den HTML-Code (unter Verwendung der DIV-Beispielabschnitte als Vorlage) ein.
   Es ist nicht erforderlich, für jede Sicherheitsdefinition DIV-Abschnitte hinzuzufügen, jedoch können nur diejenigen Definitionen mit DIV-Abschnitten in der HTML-Datei angezeigt werden, wenn diese Sicherheitslücke erkannt *und* nicht vom Sicherheitsscan repariert wurde. Sehen Sie sich hierzu den DIV-Beispieleintrag unten an.
   Sie können die zum Reparieren des Sicherheitsproblems erforderlichen Schritte, Verknüpfungen zu Software-Download-Sites sowie andere Informationen hinzufügen, die den Benutzer beim Lösen des Problems unterstützen könnten.
4. Speichern Sie Ihre Änderungen.
5. Veröffentlichen Sie geänderte HTML-Seiten erneut auf Ihren Wartungsservern.

Beispiel für einen DIV-Eintrag in einer fehlgeschlagenen (fehlerhaften) HTML-Datei.

Das nachstehende Beispiel verdeutlicht, welcher Text im Browser angezeigt wird, wenn ein Gerät den Compliance-Sicherheitsscan nicht besteht und als fehlerhaft identifiziert wurde. Dieses Beispiel basiert auf einem Textbaustein, der sich bereits in der als fehlerhaft ausgewiesenen HTML-Datei befindet. Der Text beschreibt zwei Sicherheitsdefinitionen, die nicht repariert werden konnten.

Automatisches Windows-Update (ST000003):

Schritt 1: Klicken Sie auf "Start".

Schritt 2: Klicken Sie auf die Systemsteuerung.

Schritt 3: Öffnen Sie "Automatische Updates"

Schritt 4: Klicken Sie auf "Automatisch".

Schritt 5: Klicken Sie auf OK.

Keine Antivirus Software (AV-100): Klicken Sie hier, um den Symantec Anti-Virus Client zu installieren.

Und hier ist der eigentliche HTML-Code zu diesem Beispiel:

```
<div style="display:block;clear:both;"> </div>
<div id="ttip">
<p>
<ul>
<li>Schritt 1: Klicken Sie auf "Start".</li>
<li>Schritt 2: Klicken Sie auf "Systemsteuerung".</li>
<li>Schritt 3: Öffnen Sie "Automatische Updates".</li>
<li>Schritt 4: Klicken Sie auf "Automatisch".</li>
<li>Schritt 5: Klicken Sie auf OK</li>
</ul>
</p>
</div>
```

```
<div id="ttip">
<p>
<strong>No Antivirus Software (AV-100):</strong> <a href="symantec.exe"><strong>Klicken Sie
hier</strong></a>, um den Symantec Anti-Virus Client zu installieren.
</p>
</div>
```

Suchen und Einfügen von Definitionskennungen

Die Sicherheitsdefinition wird durch den folgenden Code in der HTML-Datei identifiziert:

```
<div id="ttip">
```

Wobei "ttip" die tatsächliche Kennung der Sicherheitsdefinition ist. Sie können die Kennung einer Definition auf der Eigenschaftenseite in Patch und Compliance nachschlagen. Geben Sie die Kennung exakt so ein wie in den Eigenschaften der Definition angegeben.

Wenn die Reparatur dieser speziellen Sicherheitsdefinition fehlschlägt, wird der Inhalt des DIV-Abschnitts dynamisch im Browser des Endbenutzers angezeigt. Dem Endbenutzer werden damit nützliche Informationen zur Fehlerbehebung zur Verfügung gestellt (in dem Umfang, in dem Sie diese Informationen eingegeben haben).

Vergewissern Sie sich zunächst, dass die 802.1X NAC-Unterstützung aktiviert ist.

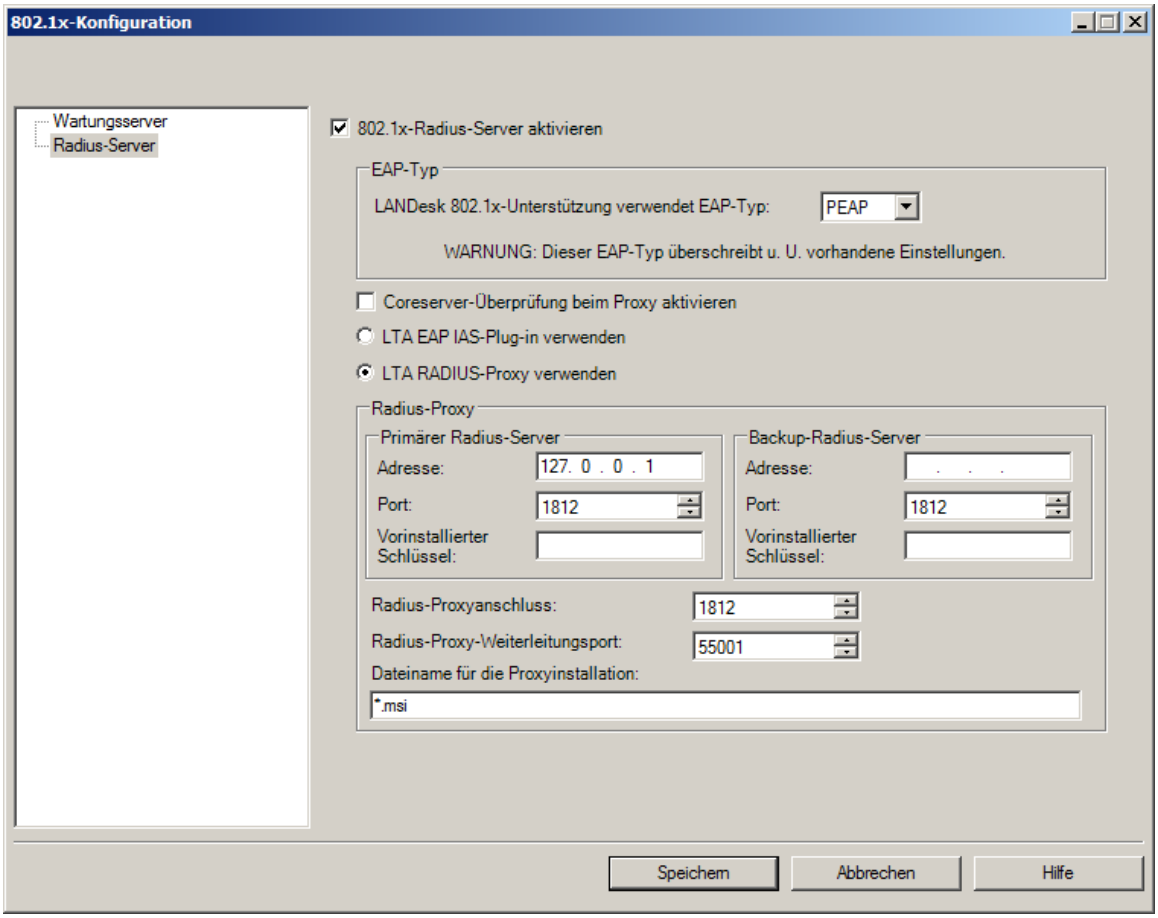
Sobald Sie die LANDesk 802.1X NAC-Unterstützung auf Ihrem Netzwerk eingerichtet und aktiviert haben (siehe nachstehende Liste) und Ihre Compliance-Sicherheitsrichtlinie definiert haben, können Sie die in den folgenden Themen beschriebenen, fortlaufenden Verwaltungsaufgaben für die Compliance-Sicherheit ausführen.

Checkliste zur Verifizierung der Aktivierung der 802.1X NAC-Unterstützung

Die LANDesk 802.1x NAC-Unterstützung ist aktiviert, wenn die folgenden Bedingungen **ALLE** erfüllt sind:

- **Gerät für die Netzwerksteuerung:** Muss ordnungsgemäß eingerichtet und konfiguriert sein; auch die erforderlichen Dienste müssen ausgeführt werden. Bei 802.1X NAC entspricht dies Ihrem Netzwerkswitch und dem 802.1X-Radius-Server.
- **Das Extra "Patch und Compliance":** Ein Benutzer mit den entsprechenden Rechten kann in der Konsole auf das Extra zugreifen. (Sie müssen über ein gültiges Security Suite-Inhaltsabonnement verfügen, mit dem Sie Sicherheitsinhalte downloaden können.)
- **Compliance-Gruppe:** Enthält mindestens eine Sicherheitsinhaltsdefinition. Der Inhalt der Gruppe "Compliance" ist der wichtigste Faktor für die Definition Ihrer Compliance-Sicherheitsrichtlinie. Die Gruppe kann Folgendes enthalten: Definitionen für Betriebssystem- und Anwendungsanfälligkeiten, Spyware-, Virenschutz- und Softwareupdates, benutzerdefinierte Definitionen und Sicherheitsbedrohungen für die Systemkonfiguration. Wenn die Gruppe "Compliance" leer ist, gibt es keine Sicherheitsinformationen, auf die das System überprüft werden kann, und somit auch keine Überprüfung des Systemzustands – mit anderen Worten, NAC wird nicht ausgeführt.
- **Reparaturserver:** Mindestens ein Wartungsserver ist eingerichtet und arbeitet ordnungsgemäß, und der Coreserver veröffentlicht Reparaturressourcen für den Wartungsserver. (Zu den Reparaturressourcen zählen der Sicherheitsclient bzw. das Dienstprogramm zum Scannen nach Anfälligkeiten, Patches im Zusammenhang mit den in der Gruppe "Compliance" enthaltenen Anfälligkeiten und die HTML Seiten, die Links zu Folgendem bereitstellen: Installieren von Trust-Agenten, Durchführen von Compliance-Sicherheitsscans sowie Reparieren erkannter Anfälligkeiten und anderer Probleme).

- **Option "802.1X Radius-Server aktivieren":** Muss im Dialogfeld **802.1x-Konfiguration** aktiviert sein.



Definieren des gewünschten Compliance-Sicherheitsniveaus

Wenn alle Bedingungen erfüllt sind, die unter "Checkliste zur Verifizierung der Aktivierung der 802.1X NAC-Unterstützung" auf Seite 572 genannt sind, dann wird die LANDesk 802.1X NAC-Unterstützung auf Ihrem Netzwerk ausgeführt.

WICHTIG: LANDesk 802.1X NAC erweitert die Sicherheit einer bestehenden 802.1X Radius-Serverumgebung
Denken Sie daran, dass das Extra "LANDesk 802.1X NAC" zur Unterstützung und als Erweiterung der Sicherheit einer *bestehenden* 802.1X Radius-Serverimplementierung in Ihrem Netzwerk gedacht ist. LANDesk 802.1X NAC ergänzt die von 802.1X bereitgestellte, einfache Zugriffssteuerung durch Funktionen zur Authentifizierung und Compliance.

Die Dienste sind flexibel angelegt und Sie können Anpassungen vornehmen, um zu beeinflussen, wie NAC Geräte handhabt (mithilfe von Optionen wie "Ausschlussliste" und "Alle zulassen"). Auch das Sicherheitsniveau kann von Ihnen angepasst werden, z. B. durch die Anzahl und Auswahl von Sicherheitsinhaltsdefinitionen, die Sie in die Gruppe "Compliance" einfügen, und indem Sie angeben, wie viele Stunden verstreichen, bevor ein Compliance-Sicherheitsscan auf Geräten, die mit dem Netzwerk verbunden sind, automatisch ausgeführt wird.

Indem Sie diese Optionen und Richtlinienkriterien anpassen, können Sie wahlweise sehr strikte und komplexe oder sehr einfache und flexible Sicherheitsrichtlinien (oder ein beliebiges Niveau dazwischen) definieren. Mit anderen Worten, Sie können beeinflussen, wie schwer oder einfach es einem Verbindungsgerät gemacht wird, den von Ihnen angegebenen Sicherheitskriterien zu entsprechen.

Und das Wichtigste ist, dass Sie die Beschaffenheit Ihrer Compliance-Sicherheitsrichtlinie jederzeit ändern können, um den sich ständig ändernden Umständen und Anforderungen zu genügen. Denken Sie daran, dass Sie bei jeder Änderung Ihrer Compliance-Sicherheitskriterien (zum Beispiel dem Inhalt der Gruppe **Compliance** in Patch und Compliance) die NAC-Einstellungen erneut auf Ihren Posture Validation- und Wartungsservern veröffentlichen müssen. Weitere Informationen finden Sie unter "Veröffentlichen von NAC-Einstellungen für Server" auf Seite 566.

Ändern und Aktualisieren von Compliance-Sicherheitsrichtlinien

Sie können Ihre Compliance-Sicherheitsrichtlinie zu jeder Zeit ändern und aktualisieren.

Sie erreichen dies, indem Sie dem Inhalt der Gruppe **Compliance** im Extra "Patch und Compliance" ändern.

Dann müssen Sie den NAC-Inhalt neu auf Posture Validation- und Wartungsservern veröffentlichen. Denken Sie daran, dass beim Veröffentlichen des NAC-Inhalts NAC-Einstellungen und Compliance-Regeln an Posture Validation-Server *und* zugehörige Patches an Wartungsserver gesendet werden; während beim Veröffentlichen von Infrastrukturdateien Setup- und Supportdateien (einschließlich Sicherheitsclient-Scanner, Trust-Agent-Installationen und HTML-Vorlagenseiten) an Wartungsserver gesendet werden. (**HINWEIS:** Im Normalfall müssen Infrastrukturdateien nur einmal auf den Wartungsservern veröffentlicht werden. Im Gegensatz zum NAC-Inhalt müssen Sie diese Dateien nicht bei jeder Änderung der Compliance-Sicherheitsrichtlinie neu veröffentlichen.

Weitere Informationen finden Sie unter "Veröffentlichen von NAC-Einstellungen für Server" auf Seite 566.

Was geschieht auf verwalteten Geräten, die mit LANDesk 802.1X NAC konfiguriert sind?

Wenn ein mit LANDesk 802.1X NAC konfiguriertes verwaltetes Gerät versucht, eine Verbindung zum Netzwerk herzustellen, läuft folgender Prozess ab:

1. Auf dem Gerät erscheint eine Anmeldeaufforderung für einen Benutzernamen und ein Kennwort.
2. Der Benutzer muss die korrekten Anmeldeinformationen für die Authentifizierung eingeben.
3. Die Anmeldeinformationen werden (zusammen mit den EAP-Daten) an den 802.1X-Radius-Server gesendet, um den Compliance-Sicherheitsscan auf dem Gerät des Endbenutzers zu initiieren.
4. Der Compliance-Sicherheitsscan bestimmt, ob das Gerät gemäß Ihrer benutzerdefinierten Sicherheitsrichtlinie fehlerfrei (compliant) oder fehlerhaft (non-compliant) ist.

   Wird das gescannte Gerät als fehlerfrei eingestuft, erhält es Zugriff auf das Unternehmensnetzwerk.

   ODER:

   Wird das gescannte Gerät als fehlerhaft eingestuft, wird es ins Quarantänenetzwerk gestellt, wo es (über den Wartungsshortcut auf dem Desktop des Geräts) repariert und erneut gescannt wird, damit ihm der Zugriff auf das Unternehmensnetzwerk gewährt werden kann.

Eine ausführlichere Beschreibung der Prozessabläufe für die Authentifizierung und Compliance und des Zusammenspiels der verschiedenen Komponenten finden Sie unter "802.1X NAC-Komponenten, Prozessablauf und Netzwerktopologie" auf Seite 545.

WICHTIG: Manuelles Zurücksetzen der 802.1X-Authentifizierung auf dem Endbenutzergerät
Wenn die Authentifizierung fehlschlägt (auch wenn Sie sicher sind, dass die richtigen Anmeldeinformationen eingegeben wurden), können Sie das lokale Netzwerk manuell zurücksetzen und einen zusätzlichen Authentifizierungsversuch durchsetzen. Klicken Sie auf dem verwalteten Gerät auf **Start > LANDesk > 802.1X zurücksetzen**.

Wenn Sie die Option "802.1X zurücksetzen" ausführen, achten Sie darauf, zuerst alle offenen Windows Popup-Dialogfelder zu schließen, sonst wird der Anmeldedialog nicht angezeigt. Wenn der Anmeldedialog zu schnell geschlossen wird, ist wahrscheinlich ein LINK-3-UPDOWN-Zustand abgelaufen. Führen Sie in diesem Fall einfach die Funktion "802.1X zurücksetzen" nochmals aus.

Anzeigen von nichtkonformen Geräten

Wenn Sie sehen möchten, auf welchen Geräten ein Posture-Vorgang ausgeführt wurde und welche dann als fehlerhaft oder nichtkonform bewertet wurden.

So zeigen Sie nichtkonforme Geräte an

1. Klicken Sie im Extra "Patch und Compliance" auf die Schaltfläche **Computer, die nicht den Vorgaben entsprechen** in der Symbolleiste. Oder Sie klicken mit der rechten Maustaste auf die Gruppe **Compliance** und klicken dann auf **Betroffene Computer**.
2. Ein Dialogfeld mit einer Liste nichtkonformer Geräte wird angezeigt.
3. Wählen Sie ein Gerät in der Liste aus, um die Sicherheitsdefinitionen anzuzeigen, gegen die das Gerät verstößt oder mit denen es nicht konform ist.

LANDesk 802.1X NAC – Fehlerbehebung

In diesem Abschnitt finden Sie Informationen über Probleme, die möglicherweise mit LANDesk 802.1X NAC entstehen können und darüber, wie Sie diese beheben können.

Geplanter Compliance-Sicherheitsscan gibt Status "Verbindung ist unterbrochen" zurück

Wenn ein geplanter 802.1X-Compliance-Sicherheitsscan-Task einen Status zurückgibt, der angibt, dass für ein Zielgerät die "Verbindung unterbrochen" oder der "Task fehlgeschlagen" ist, kann die Ursache hierfür darin liegen, dass der Taskstatus an den Coreserver gesendet wurde, während das Gerät neu gestartet wurde. Wenn Sie diesen Status sehen, können Sie das Zielgerät prüfen, um festzustellen, ob es in Quarantäne war oder nicht.

Bei einem Huawei-Switch werden mehrere 802.1X-Anmeldeaufforderungen angezeigt

Wenn Sie einen Layer 2 Huawei-Switch (H3C S3900 Serie) verwenden und ein Gerät mehr als eine 802.1X-Anmeldeaufforderung anzeigt, darf der Endanwender keine davon einfach beenden oder schließen, ohne die korrekten Nachweise einzugeben, sonst wird der 802.1X-Authentifizierungsprozess abgebrochen. In diesem Fall muss der Benutzer die richtigen Anmeldeinformationen in jedes Anmeldefenster eingeben. Wenn die Authentifizierung abgebrochen wird, verwenden Sie die Menüoption "802.1X zurücksetzen", um den Authentifizierungsprozess neu zu starten.

Bei einem Windows XP SP2-Gerät schlägt die Erstauthentifizierung nach einer Reparatur fehl

Wenn Sie ein fehlerhaftes Endbenutzergerät warten, auf dem Windows XP SP2 ausgeführt wird, und nachfolgende Authentifizierungsversuche schlagen fehl, dann können Sie die Menüoption "802.1X zurücksetzen" verwenden, um den Authentifizierungsprozess neu zu starten und erfolgreich auf das Unternehmensnetzwerk zuzugreifen.

Wenn der Radius-Server nicht verfügbar ist, kann sich das Gerät nicht authentifizieren

In Situationen, in denen der 802.1X-Radius-Server nicht für die Kommunikation mit dem LTA EAP-Agenten auf einem Endbenutzergerät zur Verfügung steht, wird das Gerät in das Quarantänenetzwerk gestellt, kann aber, da es nicht die richtige Konfiguration aufweist, weder repariert werden noch sich authentifizieren. Sie müssen warten, bis der Radius-Server verfügbar ist und dann die Menüoption "802.1X zurücksetzen" auf dem Gerät verwenden, um den Authentifizierungsprozess neu zu starten.

802.1X ist ausschließlich für Desktop-Plattformen gedacht

802.1X wird auf Server-Plattformen nicht unterstützt.

Patch und Compliance

Patch und Compliance – Übersicht

Patch und Compliance ist ein umfassendes, integriertes Extra zur Sicherheitsverwaltung, mit dem Sie Ihre mit LANDesk verwalteten Geräte vor einem breiten Spektrum von bekannten Sicherheitsrisiken und Bedrohungen schützen können.

Das Extra "Patch und Compliance" stellt alle Funktionen bereit, die Sie für den Download der gängigsten Typen von Sicherheitsinhaltsupdates (wie beispielsweise für Anfälligkeiten, Spyware, Sicherheitsbedrohungen für Konfigurationen, Virendefinitionsdateien (Musterdateien) und nicht autorisierte Anwendungen) von LANDesk Security Services benötigen. Sie können verknüpfte Patchdateien downloaden und Sicherheitsanalysen und Reparaturscans auf Ihren verwalteten Geräten konfigurieren und ausführen. Darüber hinaus können Sie eigene angepasste Definitionen erstellen, die es Ihnen ermöglichen, Ihre Geräte auf potenziell gefährliche Bedingungen zu scannen und diese Bedingungen zu beseitigen. Wenn Sicherheitsrisiken erkannt werden, können Sie betroffene Geräte mithilfe der vielfältigen Methoden von Patch und Compliance reparieren. Darüber hinaus können Sie jederzeit detaillierte Sicherheitsinformationen für gescannte Geräte einsehen und spezialisierte Patch und Compliance-Berichte erstellen.

Die Ausführung dieser unternehmensweiten Sicherheitsverwaltungsaufgaben lässt sich bequem über eine zentrale Konsole steuern.

Zusätzlich bietet Patch und Compliance Ihnen die Möglichkeit, verwaltete Geräte, Coreserver und Konsolenrechner auf installierte Versionen von LANDesk Softwareprodukten zu scannen und die entsprechenden LANDesk Softwareupdates auf diesen Geräten bereitzustellen.

HINWEIS: Informationen zu LANDesk Security Suite
Das Extra "Patch und Compliance" bildet die zentrale Komponente der Sicherheitsverwaltung von LANDesk Security Suite. Security Suite basiert vornehmlich auf den Grundfunktionen von LANDesk Management Suite, die durch spezialisierte Extras für die Sicherheitsverwaltung wie zum Beispiel Patch und Compliance, Antivirus, Endpunktsicherheit (HIPS, Firewall, Gerätesteuerung) und anderes ergänzt werden. Das Extra "Patch und Compliance" stellt in Management Suite und Security Suite dieselben Funktionen bereit und wird in diesem Abschnitt ausführlich beschrieben. Weitere Informationen dazu, welche Grundfunktionen von LANDesk in Security Suite unterstützt werden, finden Sie in den Abschnitten zu LANDesk Security Suite.

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter LANDesk Benutzercommunity – Startseite

Die nächsten Schritte: Wie es nach dem Konfigurieren von Geräten für Sicherheitsscans und Reparatur weiter geht

Sobald Sie mit den Grundkonzepten von "Patch und Compliance" vertraut sind, die Benutzeroberfläche und den allgemeinen Taskworkflow kennengelernt sowie Geräte für die Verwendung mit Patch und Compliance konfiguriert haben, können Sie die folgenden Patch- und Compliance-Verwaltungstasks ausführen. Siehe "Wesentliche Patch- und Compliancetasks im Überblick" auf Seite 581.

Verwandte Themen

- "Patch und Compliance – Funktionen und Voraussetzungen" auf Seite 579
- "Wesentliche Patch- und Compliancetasks im Überblick" auf Seite 581
- "Sicherheitsinhaltstypen und -abonnements" auf Seite 598
- "Grundlegendes zur rollenbasierten Administration mit Patch und Compliance" auf Seite 582
- "Download von Updates für Sicherheitsinhalte" auf Seite 600
- "Sicherheitsscans – Übersicht" auf Seite 620
- "Sicherheitsreparatur – Übersicht" auf Seite 631
- "Anzeigen von erkannten Sicherheitsdaten" auf Seite 628

Patch und Compliance – Funktionen und Voraussetzungen

Patch und Compliance stellt Ihnen alle Tools zur Verfügung, die Sie für die Einrichtung einer systemweiten Sicherheit in Ihrem gesamten Netzwerk benötigen. Mit Patch und Compliance lassen sich Routineprozesse im Zusammenhang mit der Verwaltung von Sicherheitsinhalten und dem Ordnen und Anzeigen dieser Inhalte automatisieren.

Analysieren Sie verwaltete Geräte mithilfe von Sicherheitsscan-Tasks und Richtlinien auf bekannte plattformspezifische Anfälligkeiten. Sie können ausführbare Patchdateien downloaden und verwalten. Schließlich können Sie erkannte Anfälligkeiten reparieren, indem Sie die vorgeschriebenen Patchdateien bereitstellen und installieren und sich von der gelungenen Durchführung eines Reparaturvorgangs überzeugen.

Sie können zudem eigene benutzerdefinierte Anfälligkeitsdefinitionen erstellen, um verwaltete Geräte auf bestimmte Betriebssystem- und Anwendungsbedingungen hin zu überprüfen, die den Betrieb und die Sicherheit Ihres Systems beeinträchtigen können. Benutzerdefinierte Definitionen können entweder nur für Erkennungsaufgaben oder sowohl für Erkennungs- als auch Reparaturaufgaben konfiguriert werden.

Grundfunktionen

Patch und Compliance unterstützt Sie bei folgenden Aufgaben:

- Realisieren von Patchsicherheit für internationale Versionen der Betriebssysteme im Netzwerk, einschließlich Unterstützung der folgenden Sprachen: Dänisch, Deutsch, Englisch, Finnisch, Französisch, Italienisch, Japanisch, Niederländisch, Norwegisch, Polnisch, Portugiesisch, Spanisch, Schwedisch, Traditionelles Chinesisch, Tschechisch und Vereinfachtes Chinesisch.
- Organisieren und Gruppieren von Sicherheitsdefinitionen zur Durchführung benutzerdefinierter Sicherheitsanalysescans und Reparaturen.
- Analysieren von Anfälligkeiten und anderen Sicherheitsrisiken auf einer Vielzahl unterstützter Plattformen, einschließlich Windows, Sun Solaris und Linux.
- Anzeigen von Patch- und Compliance-Informationen für gescannte Geräte.
- Planen automatischer Patchverwaltungsaufgaben, einschließlich Inhaltsupdates, Gerätescans und Patchdownloads.
- Reparatur als geplanter Task, Richtlinie oder automatisch über die Funktion "Automatisches Korrigieren".
- Herunterladen, Bereitstellen und Installieren von Patches, die untersucht und überprüft wurden.

- Verfolgen des Status von Patchbereitstellungen und der Installation von Patches auf gescannten Geräten.
- Verwenden der LANDesk Funktionen "Targeted Multicast", "Peer-Download" und "Checkpunkt-Neustart" für eine zügige und effiziente Patchbereitstellung.
- Generieren und Anzeigen eines breiten Spektrums von Patch und Compliance-Verwaltungsberichten.

Erweiterte Funktionen

Patch und Compliance bietet mehrere neue Merkmale. Zum Beispiel:

- Mit dem Task "Einstellungen ändern" nur die von Ihnen gewünschten Einstellungen der Konfiguration für Geräteagenten ändern/aktualisieren. Hierzu zählen: 802.1x-Unterstützungseinstellungen, Compliance-Sicherheitseinstellungen, Windows-Firewall-Einstellungen konfigurieren, Einstellungen zur Außerkraftsetzung für benutzerdefinierte Variablen, HIPS-Einstellungen, LANDesk Antivirus-Einstellungen sowie Sicherheitseinstellungen für Scannen und Reparieren. Mit dem Task "Einstellungen ändern" können die gewünschten Einstellungen geändert werden, ohne dass eine vollständige Konfiguration für Geräteagenten bereitgestellt werden muss.
- Globale Alarmeinstellungen konfigurieren.
- Auf Ihren verwalteten Geräten nach Spyware scannen. Wird Spyware erkannt, so können Sie einen Reparaturtask planen, mit dem die Spyware auf betroffenen Geräten entfernt wird.
- Mithilfe von "Definitionen für blockierte Anwendungen" den Start nicht autorisierter oder unzulässiger Anwendungen auf Endbenutzergeräten unterbinden.
- Die Echtzeit-Spyware-Überwachung (Erkennung und Entfernung) und Echtzeitanwendungsblockierung aktivieren.
- Verwaltete Geräte auf Sicherheitsbedrohungen (Fehler in der Windows-Systemkonfiguration und Schwachstellen) im lokalen Festplattenlaufwerk scannen. Sobald eine Bedrohung identifiziert wurde, können Sie die erforderliche Reparatur manuell auf dem betroffenen Gerät ausführen.
- Spezifische Sicherheitsbedrohungsdefinitionen verwenden, die die Windows-Firewall erkennen, sie ein- oder ausschalten und die Firewall-Einstellungen konfigurieren.
- Angepasste Variablen verwenden, die in anderen Sicherheitsbedrohungsdefinitionen enthalten sind, um spezifische lokale Systemkonfigurationen anzupassen und zu ändern und um unternehmensweite Systemkonfigurationsrichtlinien zu erzwingen.
- Alarmmeldungen zustellen lassen, wenn ein Sicherheitsscan bestimmte Anfälligkeiten auf verwalteten Geräten erkennt. Sie können die Alarmierung anhand des Definitionsschweregrads konfigurieren.
- Häufig auszuführende Sicherheitsscans implementieren, die schwerwiegende, zeitsensible Sicherheitsrisiken (Virenscans) aufspüren.
- Anfälligkeits- und Abhängigkeitsbeziehungen verwenden, um zu identifizieren, welche Patches installiert werden müssen, bevor andere Anfälligkeiten die verwalteten Geräte angreifen oder bevor sie repariert werden können. Ablösungsinformationen beschreiben Patches, die durch neuere Versionen ersetzt wurden und nicht angewandt werden müssen.
- Sich vergewissern, dass die neueste LANDesk Software auf Ihren verwalteten Geräten sowie Coreservern und Konsolenrechnern installiert ist, indem Sie auf LANDesk Softwareupdates scannen. Wenn der Scan ermittelt, dass auf einem Gerät eine veraltete Version installiert ist, können Sie einen Reparaturauftrag planen, mit dem das neueste LANDesk Softwareupdate bereitgestellt und installiert wird.

Unterstützte Geräteplattformen

Patch und Compliance unterstützt die meisten von LANDesk standardmäßig verwalteten Geräteplattformen, einschließlich folgender Betriebssysteme:

- Windows NT 4.0 (SP6a und höher)
- Windows 2000 Professional (SP4)
- Windows 2003 Server
- Windows XP Professional (SP1/SP2/SP3)
- Windows Vista
- Mac OS X (10.2.x, 10.3.x, und 10.4.x)
- Red Hat Linux 9 (Scannen von der Konsole aus; manuelle Reparatur)
- SUSE Linux (Scannen von der Konsole, manuelle Reparatur)
- Sun Solaris (Scannen von der Konsole, manuelle Reparatur)

Weitere Informationen zum Konfigurieren verwalteter Geräte für Sicherheitsscans finden Sie unter "Konfigurieren von Geräten für Sicherheitsscans und Reparaturen" auf Seite 593.

WICHTIG: Das Scannen von Coreservern und Konsolen auf LANDesk Softwareupdates wird unterstützt
Außerdem können Sie LANDesk Coreserver und Konsolen auf LANDesk Softwareupdates hin scannen, wobei auf diesen Geräten zuerst der Standard LANDesk Agent bereitgestellt werden muss. Dieser Agent beinhaltet den Sicherheitsscan-Agenten, der für Aufgaben, mit denen Sicherheitsscans ausgeführt werden, benötigt wird.

Verwandte Themen

"Patch und Compliance" auf Seite 578

"Wesentliche Patch- und Compliancetasks im Überblick" auf Seite 581

"Grundlegendes zur rollenbasierten Administration mit Patch und Compliance" auf Seite 582

"Download von Updates für Sicherheitsinhalte" auf Seite 600

"Sicherheitsscans – Übersicht" auf Seite 620

"Sicherheitsreparatur – Übersicht" auf Seite 631

"Anzeigen von erkannten Sicherheitsdaten" auf Seite 628

Wesentliche Patch- und Compliancetasks im Überblick

Die nachstehende Liste gibt einen Überblick über die wesentlichen Tasks zur Konfiguration, Implementierung und Verwendung von Patch und Compliance. Die funktionsspezifischen Hilfethemen liefern detaillierte Informationen zu den Konzepten, Verfahren und Prozessen.

- Konfigurieren von verwalteten Geräten für Sicherheitsscans und Reparaturen mit dem LANDesk Sicherheitsscanner-Agenten (über Agentenkonfiguration oder Installations-/Updatetasks)

- Download von Sicherheitsinhalten (Definitionen für Anfälligkeiten und andere sicherheitsbezogene Definitionen) von einem LANDesk Sicherheitsinhaltsserver (der über branchen-/anbieterspezifische Datenquellen aktualisiert wird)
- Erstellen von benutzerdefinierten Anfälligkeitsdefinitionen wie gewünscht
- Ordnen und Anzeigen von heruntergeladenen Sicherheitsinhalten
- Erstellen von Sicherheits- und Compliancebewertungsscans
- Konfigurieren von Scan- und Reparatureinstellungen zur Festlegung von Scanvorgängen und interaktiven Optionen für Endbenutzer (Diese Scan- und Reparatureinstellungen definieren Ihre Sicherheits-Compliancerichtlinien.)
- Scannen von Zielgeräten auf Anfälligkeiten, Spyware, Sicherheitsbedrohungen, blockierte Anwendungen usw. mittels benutzerdefinierten Scantasks und Einstellungen
- Anzeigen der Ergebnisse eines Sicherheitsscans für gescannte Geräte
- Download von Patches (zum Reparieren von erkannten Anfälligkeiten)
- Reparieren von erkannten Anfälligkeiten durch das Bereitstellen und Installieren von Patches auf betroffenen Geräten
- Reparieren von anderen Sicherheitslücken und -risiken auf verwalteten Geräten
- Anzeigen von Informationen zum Status der Patchinstallation und zum Reparaturverlauf
- Generieren von sicherheitsspezifischen Berichten

Verwandte Themen

"Patch und Compliance" auf Seite 578

"Patch und Compliance – Funktionen und Voraussetzungen" auf Seite 579

"Sicherheitsinhaltstypen und -abonnements" auf Seite 598

"Grundlegendes zur rollenbasierten Administration mit Patch und Compliance" auf Seite 582

"Download von Updates für Sicherheitsinhalte" auf Seite 600

"Sicherheitsscans – Übersicht" auf Seite 620

"Sicherheitsreparatur – Übersicht" auf Seite 631

"Anzeigen von erkannten Sicherheitsdaten" auf Seite 628

Grundlegendes zur rollenbasierten Administration mit Patch und Compliance

Patch und Compliance regelt den Benutzerzugriff auf Funktionen mithilfe der rollenbasierten Administration (RBA). Die rollenbasierte Administration ist das Zugriffs- und Sicherheitsmodell, mit dem LANDesk Administratoren den Zugriff der Benutzer auf Extras und Geräte steuern. Jedem Benutzer werden bestimmte Rollen und Bereiche zugewiesen, die festlegen, mit welchen Funktionen dieser Benutzer arbeiten und welche Geräte er verwalten kann.

Der Administrator weist anderen Benutzern diese Rollen mithilfe des Extras "Benutzer" in der Konsole zu. Patch und Compliance ist ein bestimmtes Recht, das im Dialogfeld "Rollen" in der Rechtegruppe "Sicherheit" aufgeführt ist. Um das Extra "Patch und Compliance" anzeigen und verwenden zu können, muss einem Benutzer das erforderliche "Patch und Compliance"-Recht erteilt werden.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Sicherheitskonfigurationen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Mit dem Patch und Compliance-Recht können Benutzer Folgendes tun:

- Das Extra "Patch und Compliance" im Menü "Extras" und in der Symbolleiste anzeigen und öffnen
- Verwaltete Geräte für die Unterstützung von Sicherheitsanalysen, Compliance- und Wartungsscans konfigurieren
- Geräte so konfigurieren, dass Echtzeitscans auf Spyware und blockierte Anwendungen zugelassen werden
- Zur Erkennung kritischer Sicherheitsrisiken Geräte für die Unterstützung von High-Frequency-Scans konfigurieren
- Sicherheitsupdates und zugehörige Patches für die Sicherheitsobjekte, für die Sie ein Security Suite-Inhaltsabonnement besitzen, downloaden
- Geplante Tasks erstellen, die Definitionen und/oder Patchupdates automatisch downloaden
- Angepasste Anfälligkeitsdefinitionen und Erkennungsregeln erstellen
- Angepasste Definitionen importieren, exportieren und löschen
- Gedownloadeten Sicherheitsinhalt nach Typ anzeigen (einschließlich: alle Typen, blockierte Anwendungen, benutzerdefinierte Definitionen, LANDesk Updates, Sicherheitsbedrohungen, Spyware, Anfälligkeiten, Treiber- und Softwareupdates)
- Ausgewählte Sicherheitsbedrohungen mit benutzerdefinierten Variablen anpassen
- Werte für benutzerdefinierte Variablen bearbeiten (für Sicherheitsinhalte mit benutzerdefinierten Variablen, z. B. Sicherheitsbedrohungen)
- Sicherheitsdefinitionen aus der Compliance-Gruppe entfernen
- Den Status von Definitionen ändern, die in der Compliance-Gruppe enthalten sind
- Sicherheits- und Compliancescans auf verwalteten Geräten als geplanten Task oder als Richtlinie konfigurieren und ausführen
- Einen Scan, der als geplanter Task ausgeführt wird, in eine Vorbereitungs- und in eine Bereitstellungsphase unterteilen
- Scan- und Reparatureinstellungen erstellen und konfigurieren, mit denen Scanoptionen festgelegt werden, wie zum Beispiel der zu scannende Inhaltstyp, die Scannerinformationen und die Statusanzeige, das Verhalten des Geräts beim Neustart und der Umfang der Interaktion mit dem Benutzer. Anschließend können Scan- und Reparatureinstellungen auf Sicherheitsscantasks, Reparaturtasks, Deinstallationstasks und Neustarttasks angewendet werden.
- Detaillierte Scanergebnisse nach erkannter Gruppe, spezifischer Definition, individuellem Gerät oder einer Gruppe ausgewählter Geräte anzeigen

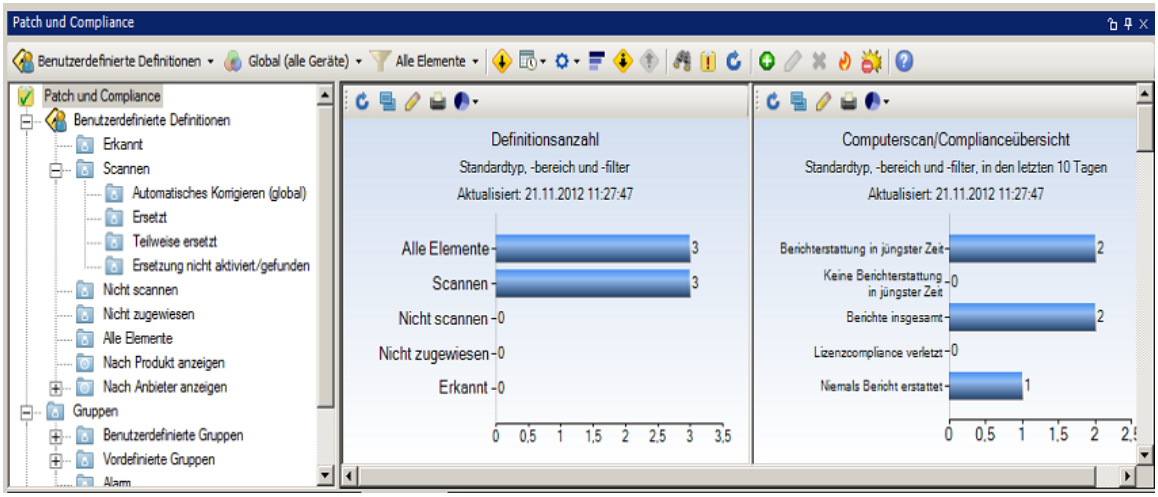
- Reparaturen als einen geplanten Task oder als Richtlinie ausführen
- Automatisches Korrigieren verwenden, um folgende Sicherheitstypen zu reparieren, falls diese erkannt werden: Anfälligkeiten, Spyware, LANDesk Softwareupdates und benutzerdefinierte Definitionen (Benutzer muss hierzu auch ein LANDesk Administrator sein)
- Den Status von Patchbereitstellungen und -installationen (Reparaturverlauf) auf gescannten Geräten nachverfolgen und überprüfen
- Nicht verwendete Typdefinitionen löschen (nur LANDesk Administratoren)
- Patches auf gescannten Geräten deinstallieren
- Patches aus der Coredatenbank entfernen
- Anfälligkeitsalarme konfigurieren
- Unterschiedliche Sicherheitsberichte generieren (hierfür wird u. a. das Rolle "Berichte" benötigt)

Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"

Das Fenster des Extras "Patch und Compliance" wird wie alle anderen Fenster von LANDesk Extras entweder über das Menü "Extras" oder die Symbolleiste geöffnet und kann mit anderen offenen Extrafenstern verankert oder unverankert sein oder über Registerkarten verfügen.

WICHTIG: Das Recht "Patch und Compliance"
Benutzer können das Extra "Patch und Compliance" nur dann sehen und darauf zugreifen, wenn Sie entweder das Recht eines LANDesk Administrators (d. h. uneingeschränkte Rechte) oder das spezifische Recht "Patch und Compliance" besitzen. Weitere Informationen über Benutzerrollen und -rechte finden Sie unter "Benutzerverwaltung" auf Seite 40.

Um das Extra "Patch und Compliance" zu öffnen, klicken Sie auf **Extras > Sicherheit und Compliance > Patch und Compliance**.



Das Patch und Compliance-Fenster enthält eine Symbolleiste und zwei Fensterausschnitte. Der linke Fensterausschnitt zeigt eine hierarchisch strukturierte Ansicht mit Sicherheitstyp-Definitionen und zu Gruppen zusammengefassten Erkennungsregeln. Sie können alle Strukturobjekte nach Bedarf erweitern oder reduzieren.

Der rechte Fensterausschnitt zeigt abhängig von der Gruppe, die Sie im linken Fensterbereich ausgewählt haben, eine Aufstellung mit den Definitions- oder Erkennungsregeldetails der ausgewählten Gruppe sowie eine Suchfunktion für die Suche in langen Elementlisten an.

HINWEIS: Zeichen, die beim Durchsuchen einer Liste nicht unterstützt werden
Im Feld **Suchen** werden die folgenden erweiterten Zeichen nicht unterstützt: <, >, ', ", !

Schaltflächen der Symbolleiste

Das Fenster des Extras "Patch und Compliance" enthält eine Symbolleiste, auf der sich folgende Schaltflächen befinden:

- **Alle Typen:**
- **Global (alle Geräte)**
- **Alle Elemente:**
- **Updates downloaden:** Öffnet ein Dialogfeld, in dem Sie die Plattformen und Sprachen für die zu aktualisierenden Sicherheitsinhaltstypen angeben können, und in dem Sie festlegen können, auf welchen Sicherheitsinhaltsserver zugegriffen werden soll. Sie können außerdem festlegen, ob Definitionen in die Gruppe "Nicht zugewiesen" eingefügt und ob verknüpfte Patches gleichzeitig heruntergeladen werden sollen. Des Weiteren können Sie den Speicherort für heruntergeladene Patches und die Proxyserver-Einstellungen angeben.
- **Task erstellen:** Enthält eine Dropdownliste, in der Sie auswählen können, welche Art von Aufgabe Sie erstellen möchten:
    - **Sicherheitsscan:** Hiermit können Sie einen Sicherheitsscantask erstellen und festlegen, ob es sich bei dem Scan um einen geplanten Task oder eine Richtlinie handelt. Sie können ferner Scan- und Reparatureinstellungen auswählen, die festlegen, ob der Sicherheitsscanner angezeigt wird, wie sich das Gerät beim Neustart verhält, welche Interaktion mit dem Benutzer erforderlich ist und welche Arten von Inhalt gescannt werden.
    - **Compliancescan:** Hiermit können Sie einen Sicherheitsscantask erstellen, der Zielgeräte gezielt auf Konformität mit Ihrer aktuellen Sicherheitsrichtlinie überprüft, wie sie in den LANDesk Network Access Control-Einstellungen und über den Inhalt der Compliance-Gruppe definiert ist. Des Weiteren können Sie angeben, ob der betreffende Compliance-Sicherheitsscan als geplanter Task (einschließlich der Festlegung der zu scannenden Geräte und der Entscheidung, ob sofort gescannt werden soll) oder als Richtlinie ausgeführt wird.
    - **Einstellungen ändern:** Hiermit können Sie einen Task erstellen, der die Standardeinstellungen auf einem verwalteten Gerät ändert, indem er die definierte Einstellungskennung in die lokale Registrierung des Geräts schreibt. Mit einem Einstellungsänderungs-Task können Sie eine oder mehrere der folgenden Einstellungen ändern: 802.1x-Unterstützungseinstellungen, Compliance-Sicherheitseinstellungen, Windows-Firewall-Einstellungen konfigurieren, Einstellungen zur Außerkraftsetzung für benutzerdefinierte Variablen, HIPS-Einstellungen, LANDesk Antivirus-Einstellungen sowie Sicherheitseinstellungen für Scannen und Reparieren. Dieser Task ist eine schnelle und praktische Möglichkeit, nur die Einstellungen zu ändern, die Sie tatsächlich ändern möchten, ohne erneut eine vollständige Geräteagentenkonfiguration bereitstellen zu müssen.

- **Neu starten:** Hiermit können Sie einen Task für einen Geräte-Neustart erstellen, angeben, ob der Neustart ein geplanter Task oder eine Richtlinie ist, sowie Scan- und Reparatureinstellungen auswählen, die das Anzeige- und Interaktionsverhalten bestimmen. Beachten Sie, dass für diesen Task nur die Optionen auf der Seite "Neu starten" des Dialogfelds gelten.
- **Reparieren:** Hiermit können Sie einen Sicherheitsreparaturtask erstellen, der erkannte Schwachstellen auf gescannten Geräten repariert. Sie können die Reparatur als geplanten Task, als Richtlinie, oder als Task und Richtlinie konfigurieren, eine Einstellung für Scannen und Reparieren definieren und Patches herunterladen. Beachten Sie, dass zum Erstellen eines Reparaturtasks zunächst mindestens eine reparierbare Sicherheitsdefinition ausgewählt werden muss.
- **Vergangenheitsdaten erfassen:** Hiermit können Sie einen Task erstellen, mit dem aktuelle Scan- und Erkennungszahlen (für eine bestimmte Anzahl von Tagen) zur Verwendung in Berichten gespeichert werden. Sie können auch einen geplanten Task erstellen und konfigurieren, der dieselbe Aktion ausführt.

- **Einstellungen konfigurieren:** Enthält eine Dropdownliste, in der Sie auswählen können, welche Einstellungen Sie konfigurieren, ändern oder aktualisieren möchten:
  - **Scan- und Reparatureinstellungen:** Hiermit können Sie Scan- und Reparatureinstellungen erstellen, bearbeiten, kopieren und löschen. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten, wie sich die Interaktion mit den Benutzern gestaltet und welche Sicherheitsinhalte gescannt werden.
  - **Compliance-Einstellungen:** Hiermit können Sie Compliance-Einstellungen erstellen, bearbeiten, kopieren und löschen. Mithilfe der Compliance-Einstellungen legen Sie fest, wann und wie ein Compliance-Sicherheitsscan durchgeführt wird, ob die Reparatur automatisch erfolgt und was zu tun ist, wenn LANDesk Antivirus einen Virenbefall auf Zielgeräten diagnostiziert.
  - **Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen:** Hiermit können Sie Scan- und Reparatureinstellungen erstellen, bearbeiten, anwenden und löschen. Durch die Außerkraftsetzung benutzerdefinierter Variablen können Sie Ausnahmen für benutzerdefinierte Variablenwerte konfigurieren. Mit anderen Worten können Sie mithilfe der Einstellungen zur Außerkraftsetzung benutzerdefinierter Variablen eine bestimmte Bedingung für eine benutzerdefinierte Variable ignorieren oder umgehen, sodass das gescannte Gerät nicht als anfällig erkannt wird.
  - **Definitionsgruppeneinstellungen:** Hiermit können Sie Definitionsgruppeneinstellungen zur Automatisierung von Downloads für Sicherheitsinhalte erstellen, bearbeiten, kopieren und löschen.
  - **Alarmeinstellungen:** Hiermit können Sie globale Sicherheitsalarme konfigurieren.
  - **Rollup Core-Einstellungen:** Hiermit können Sie Rollup-Core-Einstellungen erstellen und verwalten. Rollup Core-Einstellungen bestimmen die automatische Weiterleitung der jüngsten Sicherheitsscanergebnisse an einen Rollup-Coreserver in Ihrem Netzwerk. Durch die Weiterleitung von Sicherheitsscandaten erhalten Sie die Möglichkeit, den Anfälligkeitsstatus für Ihre sämtlichen verwalteten Geräte in einem großen verteilten Unternehmensnetzwerk in Echtzeit anzuzeigen, ohne die Daten direkt vom primären Coreserver abrufen zu müssen.

- **Benutzerdefinierte Definition erstellen:** Öffnet ein leeres Dialogfeld mit der Bezeichnung "Definitionseigenschaften". Das Dialogfeld verfügt über editierbare Felder, mit denen Sie festlegen können, ob die benutzerdefinierte Definition "nur eine Erkennung" ist oder auch Reparaturen unterstützt. Des Weiteren können Sie spezifische Anfälligkeitsinformationen eingeben, Erkennungsregeln erstellen und die entsprechende Patchdatei für den Reparaturvorgang identifizieren.
- **Benutzerdefinierte Definitionen importieren:** Hiermit können Sie eine XML-Datei importieren, die angepasste Definitionen enthält.
- **Ausgewählte benutzerdefinierte Definitionen exportieren:** Hiermit können Sie eine benutzerdefinierte Definition als XML-Datei exportieren.
- **Scaninformationen:** Hiermit können Sie für alle von Ihnen verwalteten Geräte detaillierte Informationen zu Patch und Compliance-Aktivität und -Status anzeigen, und zwar nach bestimmten Kategorien gruppiert, wie z. B. ob kürzlich gescannt oder dem Schweregrad.
- **Computer, die nicht den Vorgaben entsprechen:** Listet Geräte auf, die auf Einhaltung der vordefinierten Compliance-Sicherheitsrichtlinie gescannt wurden (basierend auf dem Inhalt der Compliance-Gruppe), und als fehlerhaft oder nicht sicherheitskonform angesehen werden.
- **Aktualisieren:** Aktualisiert den Inhalt der ausgewählten Gruppe.
- **Ausgewählte benutzerdefinierte Definitionen löschen:** Entfernt die ausgewählten benutzerdefinierten Definitionen aus der Coredatenbank.
- **Patch- und Compliancedefinitionen löschen:** Hier können Sie die Plattformen und Sprachen festlegen, deren Definitionen aus der Coredatenbank entfernt werden sollen. (**WICHTIG**: Beachten Sie, dass nur ein LANDesk Administrator diesen Vorgang ausführen kann.)
- **Hilfe:** Öffnet die Hilfe im Abschnitt über Patch und Compliance.

Dropdownliste "Typ"

Mit der Liste "Typ" legen Sie fest, welche Definitionen in der Strukturansicht heruntergeladen werden. Die Definitionstypen werden vom Herausgeber nach Inhalt zugewiesen. Das Filtern der Anzeige kann hilfreich sein, wenn Sie nur einen bestimmten Typ des Sicherheitsinhalts anzeigen oder eine extrem lange und umfassende Liste begrenzen möchten.

Die Liste "Typ" umfasst folgende Optionen:

- Alle Typen (umfassende Liste aller heruntergeladenen Sicherheitsdefinitionen)
- Antivirus (listet nur heruntergeladene Scanner-Erkennungsdefinitionen auf, keine spezifischen LANDesk Antivirus-Virendefinitionsdateien)
- Gesperrte Anwendungen (führt nur heruntergeladene, gesperrte Anwendungsdefinitionen auf)
- Benutzerdefinierte Definitionen (führt nur benutzerdefinierte Anfälligkeitsdefinitionen auf)
- Treiber-Updates (führt nur heruntergeladene Treiber-Update-Definitionen auf)
- LANDesk Updates (führt nur heruntergeladene LANDesk Softwareupdates auf)
- Sicherheitsbedrohungen (führt nur heruntergeladene Sicherheitsbedrohungsdefinitionen auf)
- Software-Updates (führt nur heruntergeladene Softwareupdates auf)
- Spyware (führt nur heruntergeladene Spywaredefinitionen auf)
- Anfälligkeiten (führt alle heruntergeladenen Anfälligkeitsdefinitionen für jede verfügbare Plattform auf)

Strukturansicht

Das Stammobjekt der Strukturansicht enthält alle Sicherheitstypen, einschließlich Anfälligkeiten, Spyware, Sicherheitsbedrohungen, blockierte Anwendungen und Gruppen mit benutzerdefinierten Definitionen (sowie entsprechende Gruppen mit Erkennungsregeln, falls zutreffend). Das Stammobjekt lässt sich nach Bedarf erweitern oder reduzieren. Die folgenden Elemente werden im linken Bereich des Fensters "Patch und Compliance" angezeigt.

Alle Typen (oder der gegenwärtig ausgewählte Typname)

Die Gruppe "Alle Typen" enthält die folgenden Untergruppen:

- **Erkannt:** Listet alle Definitionen auf, die von Sicherheitsscans für alle Geräte in diesem Scanauftrag erkannt wurden. Der Inhalt dieser Gruppe ist kumulierend, da er alle Sicherheitsscans zusammenfasst, die in Ihrem Netzwerk ausgeführt werden. Aus dieser Gruppe werden Definitionen nur durch erfolgreiche Reparatur, durch Entfernen aus der Gruppe "Scannen" und erneutes Ausführen des Scans oder durch tatsächliches Entfernen des betroffenen Geräts aus der Datenbank entfernt.

  Die Liste "Erkannt" setzt sich aus allen beim letzten Scan erkannten Sicherheitsdefinitionen zusammen. Die Spalten "Gescannt" und "Erkannt" geben an, wie viele Geräte gescannt wurden und auf wie vielen davon die Definition erkannt wurde. Wenn Sie sehen möchten, auf welchen Geräten eine Definition erkannt wurde, klicken Sie mit der rechten Maustaste auf das betreffende Element und wählen **Betroffene Computer**.

  Beachten Sie, dass Sie auch gerätespezifische Anfälligkeitsinformationen anzeigen können, indem Sie mit der rechten Maustaste auf ein Gerät in der Netzwerkansicht klicken und anschließend **Sicherheits- und Patchinformationen** wählen.

  Sie können Definitionen nur aus der Gruppe "Erkannt" in die Gruppe "Nicht zugewiesen" oder "Nicht scannen" verschieben.

- **Scannen:** (Für den Typ "Blockierte Anwendungen" heißt diese Gruppe **Verweigern**.) Listet alle Sicherheitsdefinitionen aus, nach denen beim Ausführen des Sicherheitsscanners auf verwalteten Geräten gesucht wird. Das heißt, wenn eine Definition in diese Gruppe eingefügt wird, ist sie Teil des nächsten Scanvorgangs. Andernfalls ist sie es nicht.

  Gesammelte Definitionen werden während eines Inhaltsupdates standardmäßig der Gruppe "Scannen" hinzugefügt. (**WICHTIG**: Blockierten Anwendungen werden standardmäßig zur Gruppe "Nicht zugewiesen" hinzugefügt.)

  "Scannen" ist einer von drei möglichen Zuständen einer Sicherheitsdefinition; die anderen beiden sind "Nicht scannen" und "Nicht zugewiesen". Eine Definition kann immer nur jeweils einer dieser drei Gruppen angehören. Für eine Definition gilt entweder "Scannen", "Nicht scannen" oder "Nicht zugewiesen". Für jeden Zustand gibt es ein eindeutiges Symbol (ein Fragezeichen [?] für "Nicht zugewiesen, ein rotes X für "Nicht scannen" und das reguläre Anfälligkeitssymbol für "Scannen"). Beim Verschieben einer Definition von einer Gruppe in eine andere ändert sich automatisch ihr Zustand.

  Indem Sie Definitionen in die Gruppe "Scannen" verschieben (durch Ziehen einer oder mehrerer Definitionen aus einer anderen Gruppe – mit Ausnahme der Gruppe "Erkannte Anfälligkeiten"), können Sie Art und Größe des nächsten Sicherheitsscans auf Zielgeräten bestimmen.

VORSICHT: Verschieben von Definitionen aus der Gruppe "Scannen"
Wenn Sie Definitionen aus der Gruppe "Scannen" in die Gruppe "Nicht scannen" verschieben, werden die aktuellen Informationen in der Coredatenbank, die darüber Auskunft geben, welche gescannten Geräte diese Definitionen erkannt haben, aus der Coredatenbank entfernt und stehen somit nicht mehr im Dialogfeld "Eigenschaften" einer Definition oder im Dialogfeld "Sicherheits- und Patchinformationen" eines Geräts zur Verfügung. Um diese Sicherheitsanalyse-Informationen wiederherzustellen, verschieben Sie die Definitionen wieder zurück in die Gruppe "Scannen" und führen den Scan erneut aus.

- **Nicht scannen:** (Für "Blockierte Anwendungen" ist dies die Gruppe **Nicht verweigern**.) Listet alle Definitionen auf, nach denen beim nächsten Ausführen des Sicherheitsscanners auf Geräten nicht gesucht wird. Wie oben bereits erwähnt, kann eine in dieser Gruppe enthaltene Definition nicht auch gleichzeitig in der Gruppe "Scannen" oder "Nicht zugewiesen" enthalten sein. Sie können Definitionen in diese Gruppe verschieben, um sie vorübergehend von einem Sicherheitsscan auszuschließen.
- **Nicht zugewiesen:** Listet alle Definitionen auf, die weder in die Gruppe "Scannen" noch "Nicht scannen" gehören. Die Gruppe "Nicht zugewiesen" ist im Wesentlichen ein Wartebereich für gesammelte Definitionen, bis Sie entscheiden, ob danach gescannt werden soll oder nicht.

  Sie können eine oder mehrere Definitionen aus der Gruppe "Nicht zugewiesen" durch Ziehen in die Gruppe "Scannen" oder in die Gruppe "Nicht scannen" verschieben.

  Neue Definitionen können zudem während eines Inhaltsupdates automatisch zur Gruppe "Nicht zugewiesen" hinzugefügt werden, indem Sie die Option **Neue Definitionen in die Gruppe "Nicht zugewiesen" einfügen** im Dialogfeld **Updates downloaden** auswählen.
- **Alle Elemente:** Listet alle Definitionen des ausgewählten Typs in einer einfachen Tabelle auf, selbst wenn Sie eine Definition entweder nach "Nicht zugewiesen", "Scannen" oder "Nicht scannen" verschoben haben.
- **Nach Produkt anzeigen:** Listet alle Definitionen nach Produktuntergruppen sortiert auf. Diese Untergruppen helfen Ihnen, Definitionen nach der relevanten Produktkategorie zu unterscheiden.

Sie können diese Produktuntergruppen dazu verwenden, Definitionen in die Gruppe "Scannen" für produktspezifische Scanvorgänge zu kopieren oder um sie in eine benutzerdefinierte Gruppe (siehe unten) zu kopieren, um eine Gruppe von Produkten in einem Arbeitsgang zu reparieren.

Definitionen können aus einer Produktgruppe in die Gruppe "Scannen", "Nicht scannen" oder "Nicht zugewiesen" oder in eine der benutzerdefinierten Gruppen kopiert werden. Sie können gleichzeitig in Plattform-, Produkt- und mehrfachen Kundengruppen vorkommen.

Gruppen

Das Objekt "Gruppen" umfasst die folgenden Untergruppen:

- **Benutzerdefinierte Gruppen:** Listet alle von Ihnen erstellten Untergruppen und die darin enthaltenen Definitionen auf. Mithilfe von eigenen Gruppen können Sie Sicherheitsdefinitionen Ihren eigenen Vorstellungen entsprechend organisieren. Verwenden Sie den Inhalt einer Gruppe, um mehrere Definitionen zum Durchführen benutzerdefinierter Scanvorgänge in die Gruppe "Scannen" zu kopieren, oder um einen Reparaturauftrag für mehrere Definitionen gleichzeitig zu erstellen.

  Sie können außerdem eine benutzerdefinierte Gruppe verwenden, um den Inhalt eines

Sicherheitsscans zu definieren. Kopieren Sie die Definitionen, nach denen Sie scannen möchten, in eine benutzerdefinierte Gruppe und wählen Sie diese Gruppe in der Option "Scannen für:" des Dialogfelds "Scan- und Reparatureinstellungen" aus.

Zum Erstellen einer benutzerdefinierten Gruppe klicken Sie mit der rechten Maustaste auf **Benutzerdefinierte Gruppen** (oder eine Untergruppe) und anschließend auf **Neue Gruppe**.

Um Definitionen zu einer benutzerdefinierten Gruppen hinzuzufügen, ziehen Sie eine oder mehrere Definitionen aus einer der anderen Definitionsgruppen. Sie können aber auch mit der rechten Maustaste auf eine benutzerdefinierte Gruppe klicken und anschließend auf **Definition hinzufügen** klicken.

- **Vordefiniert:** Hier werden alle vordefinierten Gruppen von Anfälligkeitsdefinitionen aufgelistet, die dem jeweiligen Abonnement für LANDesk Security Suite Sicherheitsinhalte entsprechen. Diese Gruppe könnte beispielsweise veröffentlichte Definitionen der Branche enthalten, wie zum Beispiel die "SANS Top 20", d. h. die von Microsoft erkannten und veröffentlichten Top 20 Anfälligkeitsdefinitionen. (Diese Definitionen sind in der Regel eine Teilgruppe der Microsoft Windows-Anfälligkeiten, die mit dem Dialogfeld **Updates downloaden** heruntergeladen werden.)
- **Alarm:** Listet alle Definitionen auf, die eine Alarmnachricht generieren, wenn der Sicherheitsscanner das nächste Mal auf Geräten ausgeführt wird.
- **Compliance:** Listet alle Definitionen auf, mit denen entschieden wird, ob der Zustand eines verwalteten Geräts (oder mobilen Geräts/Gastgeräts) "Fehlerfrei" oder "Fehlerhaft" ist. Diese Gruppe wird von LANDesk Network Access Control (NAC) verwendet, um den Zugriff auf das Hauptnetzwerk zu verweigern oder zuzulassen. Die Definitionen und damit verbundenen Patchdateien, die in der Gruppe "Compliance" enthalten sind, werden auf einen speziellen Reparaturserver kopiert. Dieser Server scannt Geräte, entscheidet über Compliance oder Nicht-Compliance und kann nicht konforme Geräte reparieren, damit sie vollständigen Zugriff auf das Unternehmensnetzwerk erhalten.

Erkennungsregeln

Die Gruppe "Erkennungsregeln" wird nur für bestimmte Sicherheitsinhalte angezeigt.

WICHTIG: Sicherheitsdefinitionstypen, die Erkennungsregeln verwenden
Diese Regeln definieren die spezifischen Bedingungen (des jeweiligen Betriebssystems, der Anwendung, der Datei oder Registrierung), nach der eine Anfälligkeitsdefinition sucht, um das damit verbundene Sicherheitsrisiko zu erkennen. Zu den Definitionen (d .h. Inhaltstypen), die Erkennungsregeln verwenden, zählen Anfälligkeiten, Sicherheitsbedrohungen und benutzerdefinierte Sicherheitsdefinitionen. Spyware und blockierte Anwendungen verwenden keine Erkennungsregeln.

Die Gruppe "Erkennungsregeln" enthält die folgenden Untergruppen:

- **Scannen:** Listet alle Erkennungsregeln auf, die für das Sicherheitsscannen auf Geräten aktiviert sind.

  Erkennungsregeln, die mit einer Definition für einen Sicherheitsinhalt verknüpft sind, werden während eines Inhaltsupdates standardmäßig zur Gruppe "Erkennungsregel-Scan" hinzugefügt. Auf die gleiche Weise werden benutzerdefinierte Erkennungsregeln, die mit einer benutzerdefinierten Definition verknüpft sind, beim Erstellen der benutzerdefinierten Definition zur Gruppe "Scannen" hinzugefügt.

Beachten Sie, dass die Erkennungsregeln einer Definition nicht nur aktiviert sein müssen, sondern die entsprechende ausführbare Patchdatei in einen lokalen Speicherort für Patches in Ihrem Netzwerk heruntergeladen werden muss (in der Regel auf den Coreserver), damit eine Reparatur stattfinden kann. Das Attribut "Gedownloadet" (eine der Detailspalten auf der rechten Seite im Extra-Fenster) gibt an, ob das mit dieser Regel assoziierte Patch heruntergeladen wurde.

- **Nicht scannen:** Listet alle Erkennungsregeln auf, die für das Sicherheitsscannen auf Geräten deaktiviert sind. Einige Definitionen können mit mehreren Erkennungsregeln verknüpft sein. Indem Sie eine Erkennungsregel deaktivieren, können Sie sicherstellen, dass diese nicht für das Suchen nach den Bedingungen verwendet wird, die als Hinweis dafür gelten, dass die Definition auf Geräten präsent ist. Hiermit können Sie einen Sicherheitsscan vereinfachen, ohne die Definition neu zu erstellen.
- **Nach Produkt anzeigen:** Listet alle Erkennungsregeln für gesammelte Definitionen (nach Produktuntergruppen sortiert) auf. Diese Untergruppen helfen Ihnen, Erkennungsregeln nach ihrer relevanten Produktkategorie zu unterscheiden.

Sie können diese Produktuntergruppen verwenden, um Gruppenvorgänge auszuführen.

Einstellungen

Mithilfe der Gruppe "Einstellungen" können Sie die verschiedenen Einstellungen anzeigen, die Sie für Sicherheitsscan-Tasks erstellt haben. Sie können mit der rechten Maustaste auf die Gruppe "Einstellungen" klicken, um neue Einstellungen zu erstellen und die Einstellungsinformationen in einem Berichtsformat anzuzeigen.

Enthält die folgenden Untergruppen:

- **Scannen und Reparieren:** Listet alle von Ihnen erstellten Scan- und Reparatureinstellungen auf, die für die Festlegung der Funktionsweise des Sicherheitsscanners verwendet werden. Jede Scan- und Reparatureinstellung verfügt über eine eindeutige Kennungsnummer. Der rechte Fensterausschnitt enthält nützliche Informationen zu den aufgelisteten Scan- und Reparatureinstellungen.
- **Compliance:** Listet sämtliche Compliance-Einstellungen auf, die Sie erstellt haben und die dazu verwendet werden, die Funktionsweise des Sicherheitsscanners bei der Durchführung eines Compliancescans zu bestimmen. Jede Einstellung verfügt über eine eindeutige Kennungsnummer. Der rechte Fensterausschnitt enthält nützliche Informationen zu den aufgelisteten Scan- und Reparatureinstellungen.
- **Zu überschreibende benutzerdefinierte Variablen:** Listet alle von Ihnen erstellten Einstellungen für die Außerkraftsetzung benutzerdefinierter Variablen auf; mit diesen Einstellungen wird festgelegt, welche geänderte benutzerdefinierte Variable bei der Ausführung des Sicherheitsscanners ignoriert werden soll. Jede Einstellung verfügt über eine eindeutige Kennungsnummer. Der rechte Fensterausschnitt enthält nützliche Informationen zu den aufgelisteten Einstellungen.

Definitionsdetails

Wie im Folgenden beschrieben zeigt der rechte Fensterausschnitt des Fensters "Patch und Compliance" detaillierte Informationen zu Definitions- und Erkennungsregel-Elementen in sortierbaren Spalten an.

- **Kennung:** Gibt den eindeutigen, vom Anbieter definierten alphanumerischen Code der Definition an.
- **Schweregrad:** Gibt den Schweregrad der Definition an. Mögliche Schweregrade sind: "Service Pack", "Kritisch", "Hoch", "Mittel", "Niedrig", "Nicht anwendbar" und "Unbekannt".
- **Titel:** Beschreibt Art oder Ziel der Definition in einem kurzen Text.

- **Sprache:** Gibt die Sprache des Betriebssystems oder der Anwendung an, das/die von der Definition betroffen ist.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem die Definition vom Anbieter veröffentlicht wurde.
- **Reparierbar:** Gibt an, ob sich die Definition durch Bereitstellung und Installation einer Patchdatei reparieren lässt. Zu den möglichen Werten gehören: "Ja", "Nein", "Einige" (für eine Definition, die mehrere Erkennungsregeln einschließt und bei der nicht alle erkannten Definitionen repariert werden können) und "Keine Regeln" (für eine benutzerdefinierte Definition, die keine Erkennungsregeln einschließt).
- **Unbeaufsichtigte Installation:** Gibt an, ob das zur Definition gehörende Patch (bzw. die Patches) unbeaufsichtigt, d. h. ohne Beteiligung des Benutzers installiert wird. Definitionen können u. U. mit mehreren Patches verknüpft sein. Wenn einige Patches einer Definition nicht unbeaufsichtigt installiert werden können, wird das Attribut für die unbeaufsichtigte Installation auf "Nein" gesetzt. Um zu sehen, wie einzelne Patches installiert werden, klicken Sie mit der rechten Maustaste auf die Definition und dann auf **Eigenschaften > Patches**.
- **Erkannt:** Zeigt die Zahl der gescannten Geräte an, auf denen die Definition erkannt wurde.
- **Gescannt:** Zeigt die Zahl der Geräte an, auf denen nach der Definition gesucht wurde.
- **Automatisches Korrigieren:** Gibt an, ob "Automatisches Korrigieren" für die Definition aktiviert oder deaktiviert ist.
- **CVE-Kennung:** (Gilt nur für Anfälligkeiten) Identifiziert eine Anfälligkeit anhand ihres eindeutigen CVE-Namens (CVE, Common Vulnerabilities and Exposures).

Erkennungsregeldetails

- **Name:** Zeigt den Namen der Erkennungsregel an (kann der Dateiname der ausführbaren Patchdatei sein).
- **Kennung:** Zeigt die Kennung der mit der Regel verknüpften Definition an.
- **Reparierbar:** Gibt an, ob sich die zugehörige Definition durch Bereitstellung und Installation einer Patchdatei reparieren lässt.
- **Unbeaufsichtigte Installation:** Gibt an, ob das zur Regel gehörende Patch unbeaufsichtigt, d. h. ohne Beteiligung des Benutzers installiert wird.
- **Neu starten:** Gibt an, ob die verknüpfte Patchdatei einen Neustart des Systems erforderlich macht, damit der Reparaturvorgang erfolgreich abgeschlossen wird.
- **Automatisches Korrigieren:** Gibt an, ob "Automatisches Korrigieren" für die verknüpfte Definition aktiviert oder deaktiviert ist.
- **Gedownloadet:** Gibt an, ob die mit der Regel verknüpfte ausführbare Patchdatei an den lokalen Speicherort heruntergeladen wurde.

Klicken Sie mit der rechten Maustaste auf eine Anfälligkeit, um mit der Option **Eigenschaften** weitere Details anzuzeigen. Über das Kontextmenü können Sie die Regel aktivieren/deaktivieren, den verknüpften Patch herunterladen, den Patchrepository-Ordner öffnen und den Patch deinstallieren.

Optionen und Tasks im Kontextmenü

Klicken Sie mit der rechten Maustaste auf eine Definition, um mit der Option **Eigenschaften** weitere Details anzuzeigen.

Das Kontextmenü einer Definition ermöglicht Ihnen auch die Ausführung folgender Tasks (je nach Sicherheitstyp):

- Betroffene Computer
- Computer, auf denen kein Scan ausgeführt worden ist
- Download zugehöriger Patches
- Automatisches Korrigieren beim Scannen
- Zur Compliance-Gruppe hinzufügen
- Zur Alarmgruppe hinzufügen
- Scan- bzw. Reparaturstatus löschen
- Reparieren
- Kopieren
- Eigenschaften
- Info
- Exportieren
- Auf anderen Core bzw. andere Cores kopieren
- Automatische Synchronisierung

Konfigurieren von Geräten für Sicherheitsscans und Reparaturen

Damit verwaltete Geräte auf Anfälligkeiten, Spyware, Sicherheitsbedrohungen und andere Sicherheitsrisiken gescannt werden und bereitgestellte Patches oder Softwareupdates erhalten können, muss auf ihnen der Sicherheitsscanner-Agent installiert sein (dieser Agent wird standardmäßig mit dem Standard LANDesk Agent installiert).

Dieser Abschnitt enthält Informationen zur Konfiguration von Windows-Geräten für Sicherheitsscans mittels einer Agentenkonfiguration und Informationen zur Konfiguration von Linux-, UNIX- und Mac-Geräten.

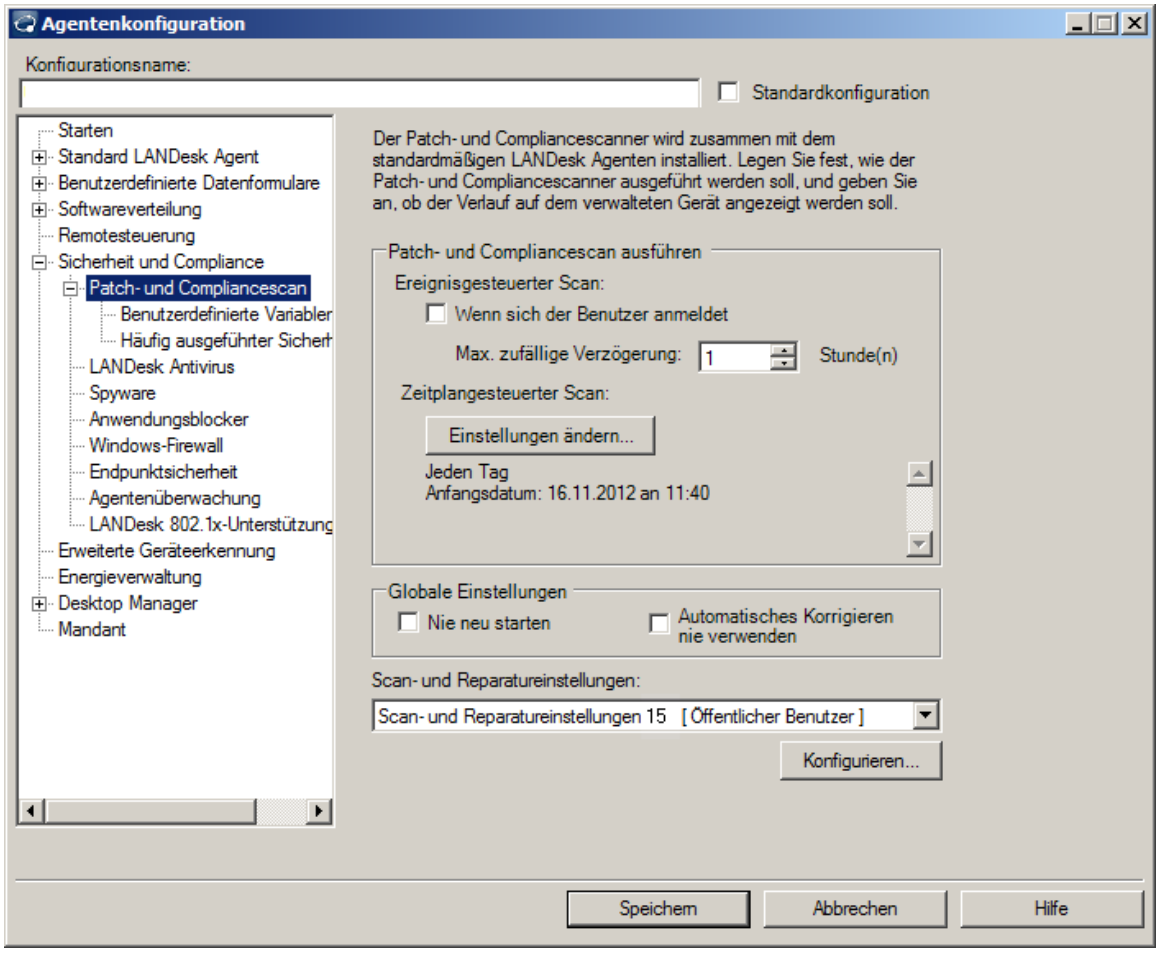
HINWEIS: Das Scannen von Coreservern und Konsolen auf LANDesk Softwareupdates wird unterstützt
Außerdem können Sie LANDesk Coreserver und Konsolen auf LANDesk Softwareupdates hin scannen, wobei auf diesen Geräten zuerst der Standard LANDesk Agent bereitgestellt werden muss. Dieser Agent beinhaltet den Sicherheitsscan-Agenten, der für Aufgaben, mit denen Sicherheitsscans ausgeführt werden, benötigt wird.

Konfigurieren von Windows-Geräten für Sicherheitsscans

Jetzt ist Sicherheitsscanner-Agent standardmäßig Teil des LANDesk Standardagenten und wird selbst auf Geräten installiert, die nur über eine rudimentäre Agentenkonfiguration verfügen. Mit anderen Worten, jedes mit dem neuen Agentenkonfigurationstool konfigurierte Windows-Gerät ist auf die Patch und Compliancescans und die entsprechenden Reparaturvorgänge vorbereitet.

Konfigurieren von Geräten mit dem Extra "Agentenkonfiguration"

Das Extra "Agentenkonfiguration" (**Extras > Konfiguration > Agentenkonfiguration > Neue Windows-Konfiguration**) verwenden Sie zur Erstellung von Agentenkonfigurationen mit bestimmten Patch und Compliance-Scaneinstellungen und anderen Sicherheitseinstellungen, die für Zielgeräte bereitgestellt werden können.



So konfigurieren Sie Geräte mit einer Agentenkonfiguration für Sicherheitsscans und Reparaturen

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie in der Symbolleistenschaltfläche auf **Neues Windows**.
3. Nachdem Sie die gewünschten Einstellungen für die Agentenkonfiguration festgelegt haben, klicken Sie auf die Gruppe **Sicherheit und Compliance** und dann auf **Patch- und Compliancescan**.
4. Wählen Sie, wie der Sicherheitsscanner auf Ihren verwalteten Geräten ausgeführt werden soll. Für weitere Informationen zu einer Option klicken Sie auf **Hilfe**.

5. Wählen Sie eine Scan- und Reparatureinstellung aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können eine neue Einstellung erstellen oder eine vorhandene bearbeiten, indem Sie auf **Konfigurieren** klicken. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten, wie sich die Interaktion mit den Benutzern gestaltet und welche Sicherheitsinhalte gescannt werden.
6. Legen Sie alle anderen gewünschten Einstellungen für die Agentenkonfiguration fest und klicken Sie dann auf **Speichern**.

Beim Erstellen oder Bearbeiten einer Agentenkonfiguration können Sie bestimmte Optionen des Sicherheitsscanners konfigurieren. So können Sie beispielsweise bestimmen, wann und wie oft der Scanner auf verwalteten Geräten automatisch ausgeführt wird, ob der Scanverlauf angezeigt und ob Abfragen auf dem Gerät des Endanwenders eingeblendet werden. Darüber hinaus können Sie globale Einstellungen für Reparaturaktionen festlegen, beispielsweise in Bezug auf den Neustart von Geräten und die Durchführung automatischer Reparaturvorgänge. Wenn Sie mehr darüber erfahren möchten, wie Sie das Verhalten des Sicherheitsscanner-Agenten im Rahmen der Erstellung und Bereitstellung von Agentenkonfigurationen an verwaltete Windows-Geräte anpassen können, lesen Sie die Informationen unter "Bereitstellen von LANDesk Sicherheitsdiensten" auf Seite 133.

HINWEIS: Auf Windows 9x-Geräten wird WinSock2 für die Ausführung des Sicherheitsscanner-Agenten benötigt.

Im Anschluss an die Agentenkonfiguration wird auf dem verwalteten Gerät ein Programmsymbol für den Sicherheitsscanner zur Programmgruppe **LANDesk Management** im **Start**menü hinzugefügt. Dieses Programm kann dazu verwendet werden, den Scanner direkt von dem Gerät aus auszuführen (statt diesen per "Run"-Schlüssel oder wiederkehrend mit dem Local Scheduler oder über einen geplanten Task von der Konsole aus zu starten).

Zusätzliche Sicherheitseinstellungen in Agentenkonfigurationen

Beim Definieren einer Geräte-Agentenkonfiguration (für Windows-Geräte) können Sie auch die folgenden ergänzenden Sicherheitsfunktionen aktivieren und konfigurieren:

- Häufiges Sicherheitsscanning nach schwerwiegenden Sicherheitsrisiken
- Spywareüberwachung
- Anwendungsblocker
- Windows-Firewall
- Endpunktsicherheit mit folgenden Sicherheitskomponenten: HIPS, LANDesk Firewall und Gerätesteuerung
- Agentenüberwachung für die Überwachung von Dateien und Diensten
- 802.1X NAC-Unterstützung, mit der die Netzwerkzugriffssteuerung (NAC) durch Authentifizierung und Compliance erweitert wird

Weitere Informationen finden Sie in den Abschnitten unten.

Informationen zur Seite "Häufig ausgeführter Sicherheitsscan"

Verwenden Sie diese Seite, um Systeme mit einem High Frequency Scanner auf kritische, zeitsensible Risiken zu überprüfen, beispielsweise neu erkannte und bösartige Viren sowie Risiken im Zusammenhang mit der Firewall-Konfiguration.

Diese Seite enthält folgende Optionen:

- **Häufig ausgeführten Sicherheitsscan verwenden:** Aktiviert einen häufig ausgeführten Sicherheitsscan auf Geräten mit dieser Agentenkonfiguration.
- **Nur Scannen, wenn Benutzer angemeldet ist:** Schränkt den häufigen Sicherheitsscan insofern ein, als dieser nur ausgeführt wird, wenn auf dem Zielgerät ein Benutzer angemeldet ist.
- **Alle:** Gibt das Zeitintervall für einen häufig ausgeführten Sicherheitsscan an.
- **Scan- und Reparatureinstellungen (die nach einer Gruppe suchen):** Gibt die Scan- und Reparatureinstellungen an, die den Sicherheitsscanner für häufig ausgeführte Sicherheitsscans steuern. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten und wie sich die Interaktion mit den Benutzern gestaltet. Die von Ihnen ausgewählte Einstellung muss für das Scannen von Gruppen (nicht Typen) konfiguriert werden. Sie können auch auf **Konfigurieren** klicken, um eine neue Scan- und Reparatureinstellung zu erstellen, die mit einer Gruppe verknüpft ist.

Informationen zu den Seiten "Spyware" und "Anwendungsblocker"

Diese Seiten verwenden Sie, um das Verweigern von Anwendungen in Echtzeit und das Erkennen sowie Löschen von Spyware in Echtzeit auf verwalteten Geräten, auf die diese Agentenkonfiguration angewendet wurde, zu aktivieren und zu konfigurieren.

WICHTIG: Rechtshinweis bezüglich blockierter Anwendungen
Rechtliche Hinweise bezüglich blockierter Anwendungsinhalte finden Sie unter "Rechtshinweis zum Typ "Blockierte Anwendung"" auf Seite 611.

Die Spyware-Erkennung in Echtzeit sucht nur nach Spyware-Definitionen, die sich in der Gruppe **Scannen** befinden und für die "Automatisches Korrigieren" eingeschaltet ist. Sie können die Option "Automatisches Korrigieren" für heruntergeladene Spyware-Definitionen entweder automatisch aktivieren oder Sie können Spyware-Definitionsupdates konfigurieren, sodass die Option "Automatisches Korrigieren" beim Download der Definitionen automatisch aktiviert wird.

Die Spyware-Erkennung in Echtzeit überwacht Geräte auf neu gestartete Prozesse, die versuchen, die lokale Registrierung zu manipulieren. Wenn Spyware erkannt wird, fordert der Sicherheitsscanner des Geräts den Endanwender auf, die Spyware zu entfernen.

Diese Seite enthält folgende Optionen:

- **Echtzeit-Spywareblockierung aktivieren:** Aktiviert Spyware-Überwachung und Blockierung in Echtzeit auf Geräten, die über diese Agentenkonfiguration verfügen.

  HINWEIS: Damit das Echtzeit-Spyware-Scanning und die Spyware-Erkennung funktioniert, müssen Sie die automatische Korrekturfunktion manuell aktivieren, um die heruntergeladenen Spyware-Definitionen im Sicherheitsscan einzuschließen. Die automatische Reparaturfunktion ist für heruntergeladene Spyware-Definitionen standardmäßig nicht eingeschaltet.

- **Benutzer benachrichtigen, wenn Spyware blockiert wurde:** Zeigt eine Meldung an, die den Endanwender informiert, dass ein Spyware-Programm erkannt und repariert wurde.
- **Wenn eine Anwendung nicht als Spyware erkannt wird, die Genehmigung des Benutzers für die Installation anfordern:** Selbst wenn der erkannte Prozess nicht als Spyware eingestuft wird (gemäß der aktuellen Liste der Spyware-Definitionen für dieses Gerät), wird der Benutzer dennoch zur Bestätigung aufgefordert, bevor die Software auf dem Computer installiert wird.

Bei Verwendung der Anwendungsblockierung in Echtzeit ist die Reparatur KEIN separater Task. Das Verweigern einer Anwendung findet als Teil des eigentlichen Sicherheitsscans statt, indem die Registrierung auf dem lokalen Festplattenlaufwerk so bearbeitet wird, dass der Benutzerzugriff auf diese nicht autorisierten Anwendungen deaktiviert wird. Die Sicherheitsdienste verwenden das Programm "softmon.exe", um den Zugriff auf spezifische Programmdateien zu verweigern, selbst wenn der Name der ausführbaren Datei geändert wurde, da softmon.exe die Dateiheader-Informationen liest.

Diese Seite enthält folgende Optionen:

- **Blockierung der unzulässigen Anwendungen aktivieren:** Aktiviert Anwendungsblockierung in Echtzeit auf Geräten, die über diese Agentenkonfiguration verfügen.
- **Benutzer benachrichtigen, wenn eine Anwendung blockiert wurde:** Zeigt eine Meldung an, die den Benutzer informiert, dass er versucht hat, eine unzulässige Anwendung zu starten, und dass der Zugriff verweigert wurde.

Konfigurieren von Linux- und UNIX-Geräten für Sicherheitsscans

Patch und Compliance unterstützt Anfälligkeitsscans auch auf folgenden Systemen:

- Red Hat Linux
- SUSE Linux
- Sun Sparc (Solaris 8)

Für jede Plattform können mit Patch und Compliance Sicherheitsinhalte heruntergeladen werden, so wie dies auch bei Windows-Anfälligkeiten der Fall ist.

Linux- und UNIX-Geräte können nicht mit dem Sicherheitsscanner-Agenten über das Extra "Agentenkonfiguration" der Konsole konfiguriert werden. Unter Linux und UNIX ist die Gerätekonfiguration ein manueller Prozess.

Weitere Informationen zur Einrichtung von Linux- und UNIX-Geräten finden Sie unter "Konfigurieren von Linux- und UNIX-Geräteagenten" auf Seite 118.

Sie können auch die README-Datei zu Rate ziehen, die sich in der entsprechenden .tar-Datei der jeweiligen Plattform im zugehörigen Plattformordner unter ManagementSuite\LDLogon auf dem Coreserver befindet.

Sobald Linux- und UNIX-Plattformen konfiguriert sind, können sie über geplante Tasks von der Konsole aus auf Anfälligkeiten gescannt werden. Werden Anfälligkeiten erkannt, so muss die Reparatur manuell auf dem betroffenen Gerät durchgeführt werden.

Konfigurieren von Mac OS X-Geräten für Sicherheitsscans

Auf Macintosh OS X-Geräten unterstützt Patch und Compliance jetzt sowohl den Download von Sicherheitsinhalten als auch Sicherheitsscans und Reparaturen.

Außerdem können Sie mit dem Agentenkonfigurationstool Agentenkonfigurationen für Ihre Macintosh-Geräte erstellen und konfigurieren. Wie bei der Windows-Agentenkonfiguration ist der Sicherheitsscanner-Agent auch für Macintosh-Geräte Teil des Standard LANDesk Agenten.

Nähere Informationen zur Erstellung und Bereitstellung einer Macintosh-Agentenkonfiguration mit Sicherheitsscanner-Unterstützung finden Sie unter "Verwalten von Macintosh-Geräten" auf Seite 505.

Sobald die Macintosh-Geräte konfiguriert sind, können sie über geplante Tasks von der Konsole aus auf Anfälligkeiten gescannt werden. Werden Anfälligkeiten erkannt, so muss die Reparatur auf dem betroffenen Gerät durchgeführt werden.

So starten Sie den Sicherheitsscanner manuell auf Mac-Geräten

1. Öffnen Sie die **Systemeinstellungen** von MAC OS X und wählen Sie die Seite **LANDesk Client**.
2. Klicken Sie auf der Registerkarte **Übersicht** auf **Jetzt prüfen** im Abschnitt **Sicherheit**.

Sicherheitsinhaltstypen und -abonnements

Im Installationspaket der LANDesk Management Suite ist jetzt auch standardmäßig das Extra "Patch und Compliance" enthalten (bisher wurde dieses Tool als separates Add-On zur Verfügung gestellt). Ohne Security Suite-Inhaltsabonnement können Sie jedoch nur auf LANDesk Softwareupdates und angepasste Definitionen scannen. Mit einem Security Suite-Inhaltsabonnement können Sie das Extra "Patch und Compliance" vollständig nutzen, da Sie hiermit Zugriff auf zusätzliche Sicherheitsinhalte (Definitionstypen) erhalten.

Folgende Arten von LANDesk Security Suite Sicherheitsinhalten gibt es:

- Antivirus-Updates (schließt für Scanner anderer Hersteller nur vom Antivirus-Scanner erkannten Inhalt ein; schließt für LANDesk Antivirus sowohl vom Scanner erkannten Inhalt als auch Virendefinitionsdateien ein)
- Blockierte Anwendungen (siehe "Rechtshinweis zum Typ "Blockierte Anwendung"" auf Seite 611)
- Benutzerdefinierte Anfälligkeitsdefinitionen
- Treiberupdates
- LANDesk Softwareupdates
- Sicherheitsbedrohungen (Schwachstellen der Systemkonfiguration; umfasst Firewallerkennung und -konfiguration)
- Softwareupdates
- Spyware
- Anfälligkeiten (bekannte Plattform- und anwendungsspezifische Anfälligkeiten)

Informationen zu den Security Suite-Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.

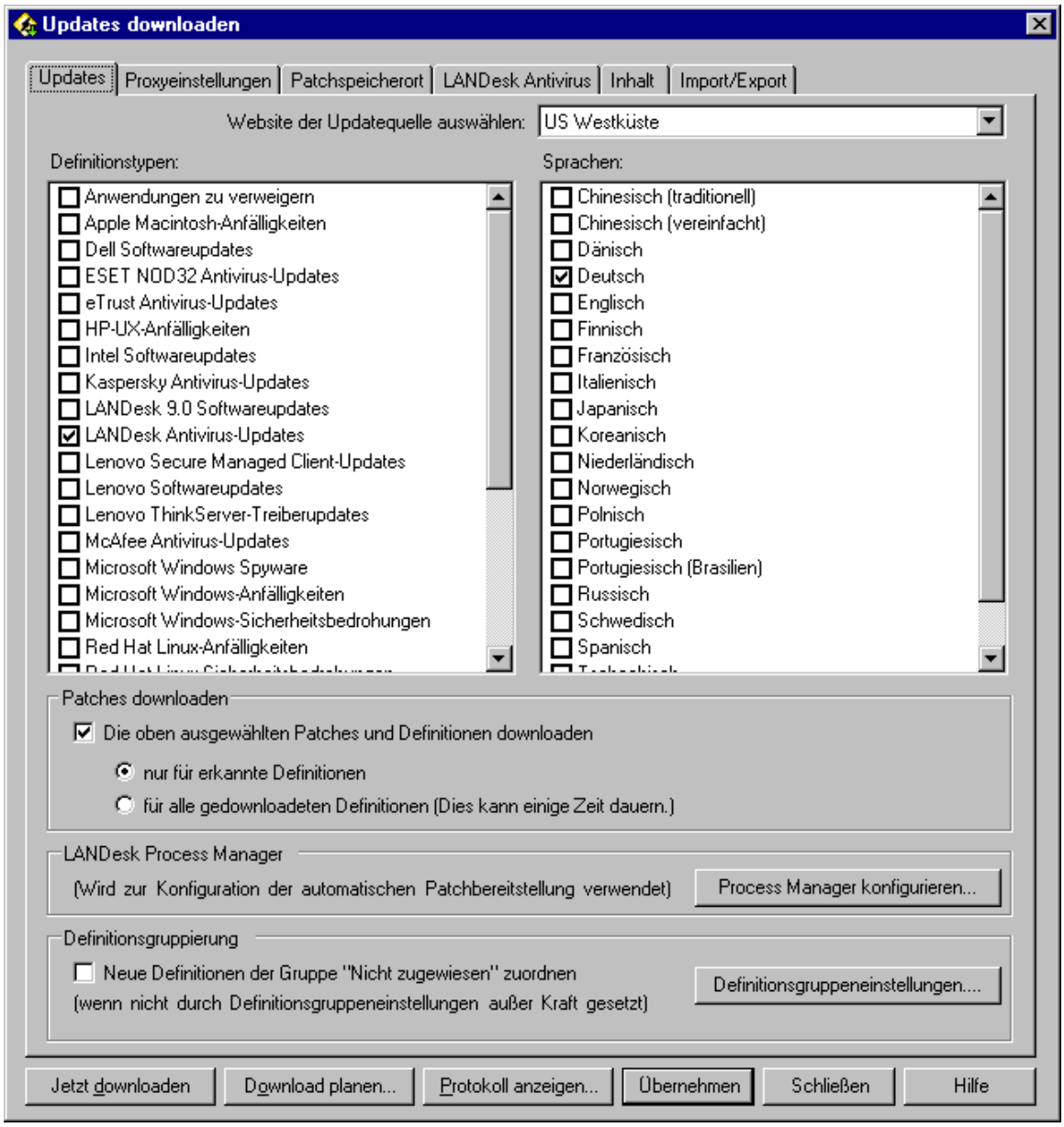
LANDesk Startseite

Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter

LANDesk Benutzercommunity – Startseite

Download von Updates

Beachten Sie, dass die Seite **Updates** im Dialogfeld **Updates downloaden** mehrere Sicherheitsinhaltstypen in der Liste der Definitionstypen enthält.



Scan- und Reparaturfunktionen sind bei diesen unterschiedlichen Inhaltstypen nicht identisch. Nähere Informationen dazu, wie Patch und Compliance auf verwalteten Geräten nach den verschiedenen Typen von Sicherheitsrisiken scannt und diese repariert, finden Sie in den entsprechenden Abschnitten unter "Sicherheitsscans – Übersicht" auf Seite 620.

Verwandte Themen

"Patch und Compliance" auf Seite 578

"Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584

"Download von Updates für Sicherheitsinhalte" auf Seite 600

"Herunterladen von Patches" auf Seite 609

"Anzeigen und Ordnen von Sicherheitsinhalten" auf Seite 604

"Sicherheitsscans – Übersicht" auf Seite 620

"Sicherheitsreparatur – Übersicht" auf Seite 631

Download von Updates für Sicherheitsinhalte

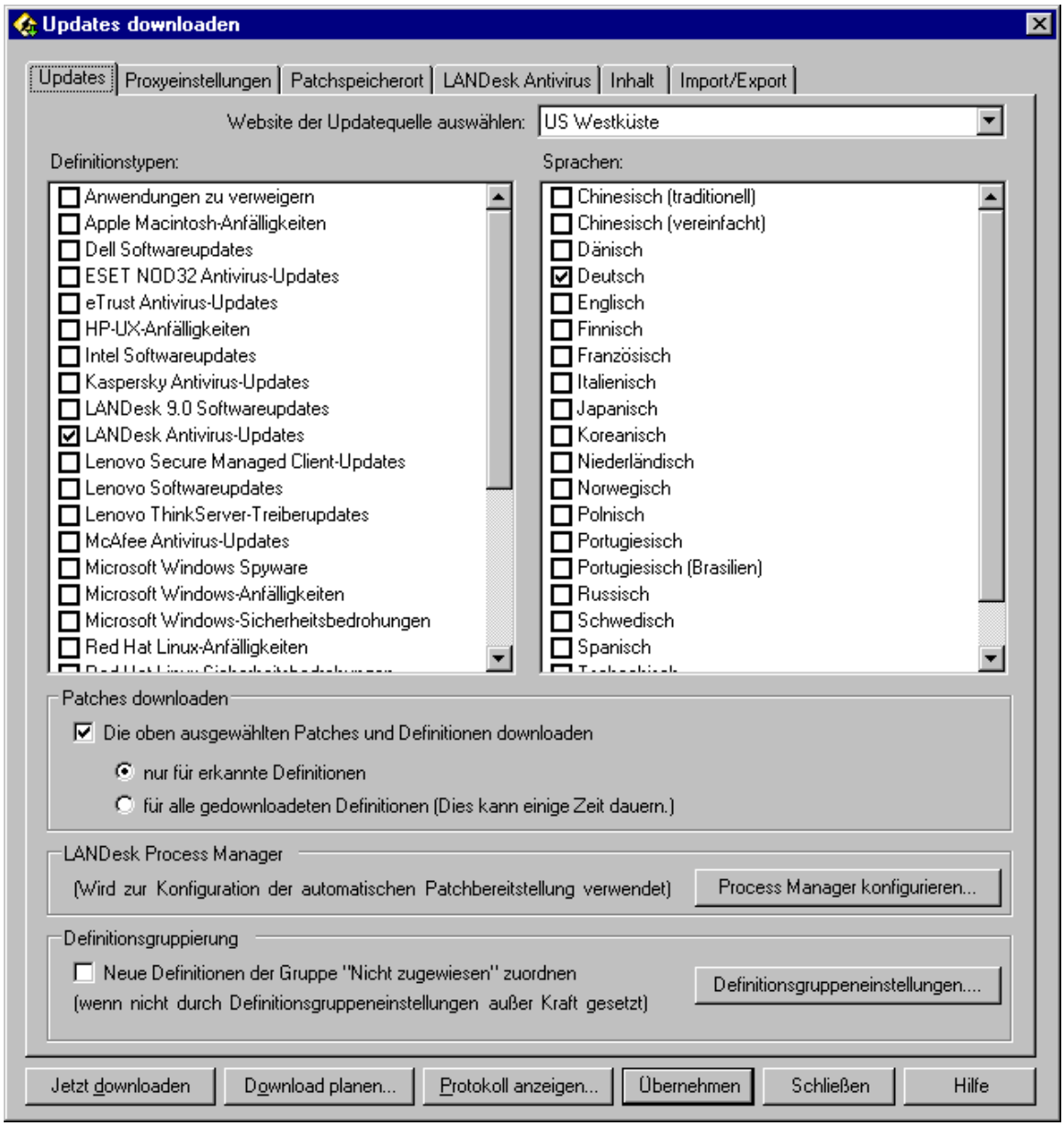
Ihr Netzwerk und Ihre Geräte sind ständig Bedrohungen und Sicherheitsrisiken ausgesetzt, z. B. durch Würmer, Viren und Spyware sowie Gefahren im Zusammenhang mit der Systemwartung (Softwareaktualisierungen, Bugfixes etc.). Patches werden in regelmäßigen Abständen veröffentlicht, um Anwendern die Möglichkeit zu geben, unvermeidbare Betriebssystem- und Anwendungsanfälligkeiten zu reparieren. Das Extra "Patch und Compliance" vereinfacht und beschleunigt den Prozess des Abrufens der neuesten Definitionen und Patches, indem es Ihnen die Möglichkeit gibt, Inhalte über eine von LANDesk bereitgestellte Datenbank herunterzuladen. Der LANDesk Security Suite Dienst konsolidiert bekannte Definitionen, die aus vertrauenswürdigen Quellen der Industrie und des Handels abgerufen werden, und leitet zuverlässige Informationen direkt an Sie weiter.

HINWEIS: Patch und Compliance unterstützt auch benutzerdefinierte Anfälligkeitsdefinitionen
Zusätzlich zu den bekannten Anfälligkeiten können Sie eigene Anfälligkeitsdefinitionen und damit verknüpfte Erkennungsregeln erstellen. Weitere Informationen finden Sie unter "Benutzerdefinierte Sicherheitsdefinitionen – Übersicht" auf Seite 612.

Die Einrichtung und Verwaltung aktueller Sicherheitsinhalte hat folgende Vorteile: Art und Umfang von Sicherheitsrisiken für jede von Ihnen unterstützte Plattform und Anwendung lassen sich besser einschätzen, Sie können leichter bestimmen, welche Anfälligkeiten und anderen Risiken für Ihre Umgebung relevant sind und Sicherheitsscan- sowie Reparaturaufgaben können problemlos angepasst werden. Die Umsetzung dieser Strategie für die Sicherheitsverwaltung beginnt damit, dass Sie eine aktuelle Liste mit den neuesten bekannten Sicherheitsinhalten downloaden.

Download von Updates

Mit dem Dialogfeld "Updates downloaden" (**Extras > Sicherheit > Patch und Compliance > Updates downloaden**) können Sie Updates für Sicherheitsinhalte konfigurieren und diese sofort durchführen oder einen geplanten Updatetask erstellen, der zu einem bestimmten Zeitpunkt oder als wiederkehrender Task ausgeführt werden soll (siehe "Planen von automatischen Updates für Sicherheitsinhalte" auf Seite 604).



VORSICHT: Pro Coreserver (einschließlich zusätzlicher Konsolen) kann immer nur jeweils ein LANDesk Benutzer Sicherheitsinhalte aktualisieren. Wenn ein Benutzer versucht, Inhalte zu aktualisieren, während der Prozess bereits läuft, wird eine Meldung angezeigt, die auf einen vorhandenen Konflikt hinweist.

So downloaden Sie Sicherheitsinhalte (und Patches)

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Updates downloaden**.
3. Wählen Sie die Website für die Updatequelle in der Liste der verfügbaren Content-Server aus.

4. Wählen Sie die Definitionstypen aus, deren Sicherheitsinhalt Sie aktualisieren möchten. Sie können einen oder mehrere Typen aus der Liste auswählen (je nach LANDesk Security Suite-Inhaltsabonnement). Je mehr Typen Sie auswählen, umso länger dauert die Aktualisierung.
5. Wählen Sie die Sprachen aus, deren Inhalt Sie für die von Ihnen angegebenen Typen aktualisieren möchten.

   Einige Anfälligkeiten und Definitionstypen sowie damit verknüpfte Patches sind sprachneutral oder unabhängig, d. h., sie sind mit jeder Sprachversion des Betriebssystems oder Anwendung kompatibel, die von dieser Definition adressiert wird. Sie benötigen demnach keinen eindeutigen sprachspezifischen Patch, um diese Anfälligkeiten zu reparieren, da das Patch alle unterstützten Sprachen abdeckt. Linux-und UNIX-Plattformen verwenden beispielsweise nur sprachneutrale Definitionen und Patches. Microsoft Windows und Apple Macintosh verwenden jedoch fast ausschließlich sprachspezifische Anfälligkeitsdefinitionen und Patches.

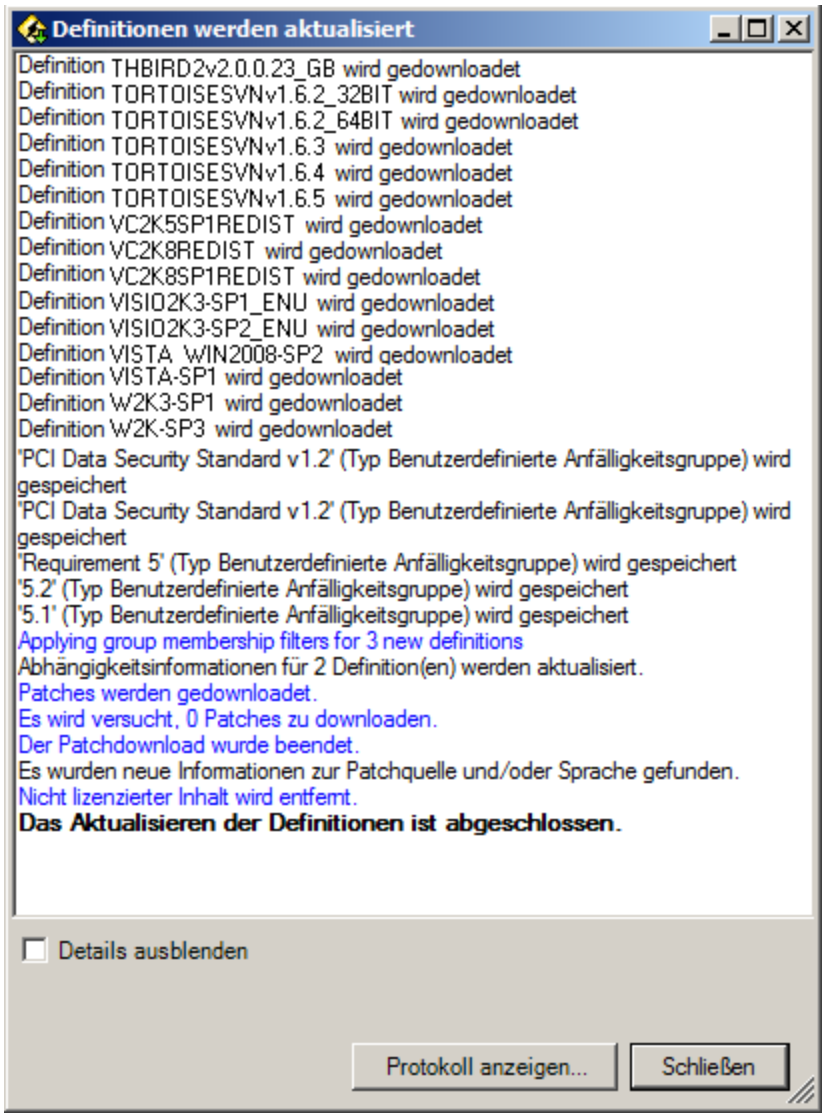
   Beim Herunterladen des Inhalts für eine bestimmte Plattform (mit dem entsprechenden Abonnement) werden per Standardeinstellung alle sprachneutralen Anfälligkeitsdefinitionen der ausgewählten Plattform automatisch aktualisiert. Wenn Sie einen Windows- oder Mac-Inhaltstyp ausgewählt haben, müssen Sie zudem die Sprachen auswählen, deren Definitionen Sie aktualisieren möchten. Wenn Sie die Sun Solaris- oder eine Linux-Plattform ausgewählt haben, müssen Sie keine Sprache auswählen, da ihr Inhalt sprachneutral ist und automatisch aktualisiert wird.

6. Wenn Sie veranlassen möchten, dass neuer Inhalt (d. h. Inhalt, der noch nicht in einer der Gruppen existiert) automatisch in die Gruppe "Nicht zugewiesen" eingefügt wird, anstatt in den Standardspeicherort (die Gruppe "Scannen"), aktivieren Sie das Kontrollkästchen **Neue Definitionen in die Gruppe "Nicht zugewiesen" einfügen**.
7. Wenn Sie verknüpfte ausführbare Patchdateien automatisch downloaden möchten, aktivieren Sie das Kontrollkästchen **Patches downloaden** und klicken anschließend auf eine der folgenden Downloadoptionen. (**HINWEIS:** Die Patches werden in den Speicherort heruntergeladen, der auf der Seite **Patchspeicherort** des Dialogfelds "Updates downloaden" angegeben wurde.

   - **Nur für erkannte Definitionen:** Downloadet nur die Patches, die mit Anfälligkeiten, Sicherheitsbedrohungen oder LANDesk Updates verknüpft sind, die vom letzten Sicherheitsscan erkannt wurden (d. h. die Definitionen, die sich derzeit in der Gruppe "Erkannt" befinden).
   - **Für alle gedownloadeten Definitionen:** Lädt ALLE Patches herunter, die mit Anfälligkeiten, Sicherheitsbedrohungen und LANDesk Updates verknüpft sind, die sich derzeit in der Gruppe "Scannen" befinden.

8. Wenn Ihr Netzwerk über einen Proxyserver verfügt, der für externe Internet-Übertragungen verwendet wird (für die Aktualisierung von Sicherheitsinhalten und den Download von Patches erforderlich), klicken Sie auf die Registerkarte **Proxyeinstellungen** und geben die Serveradresse, Portnummer sowie Anmeldeinformationen ein, wenn für den Zugriff auf den Proxyserver eine Anmeldung erforderlich ist.
9. Klicken Sie auf **Übernehmen**, wenn Sie die Einstellungen speichern möchten.

10. Klicken Sie auf **Jetzt aktualisieren**, um das Update für die Sicherheitsinhalte auszuführen. Das Dialogfeld **Definitionen werden aktualisiert** (siehe unten) zeigt den aktuellen Vorgang und Status an. (Klicken Sie auf **Update planen**, um einen geplanten Task zu erstellen)
11. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Schließen**. Wenn Sie auf **Abbrechen** klicken, bevor die Aktualisierung abgeschlossen ist, werden nur die bis zu diesem Zeitpunkt verarbeiteten Sicherheitsinhalte in die Coredatenbank heruntergeladen. Sie müssen die Aktualisierung erneut ausführen, um den restlichen Sicherheitsinhalt abzurufen.


Definitionen werden aktualisiert
Definition THBIRD2v2.0.0.23_GB wird gedownloadet
Definition TORTOISESVNv1.6.2_32BIT wird gedownloadet
Definition TORTOISESVNv1.6.2_64BIT wird gedownloadet
Definition TORTOISESVNv1.6.3 wird gedownloadet
Definition TORTOISESVNv1.6.4 wird gedownloadet
Definition TORTOISESVNv1.6.5 wird gedownloadet
Definition VC2K5SP1REDIST wird gedownloadet
Definition VC2K8REDIST wird gedownloadet
Definition VC2K8SP1REDIST wird gedownloadet
Definition VISIO2K3-SP1_ENU wird gedownloadet
Definition VISIO2K3-SP2_ENU wird gedownloadet
Definition VISTA_WIN2008-SP2 wird gedownloadet
Definition VISTA-SP1 wird gedownloadet
Definition W2K3-SP1 wird gedownloadet
Definition W2K-SP3 wird gedownloadet
'PCI Data Security Standard v1.2' (Typ Benutzerdefinierte Anfälligkeitsgruppe) wird gespeichert
'PCI Data Security Standard v1.2' (Typ Benutzerdefinierte Anfälligkeitsgruppe) wird gespeichert
'Requirement 5' (Typ Benutzerdefinierte Anfälligkeitsgruppe) wird gespeichert
'5.2' (Typ Benutzerdefinierte Anfälligkeitsgruppe) wird gespeichert
'5.1' (Typ Benutzerdefinierte Anfälligkeitsgruppe) wird gespeichert
Applying group membership filters for 3 new definitions
Abhängigkeitsinformationen für 2 Definition(en) werden aktualisiert.
Patches werden gedownloadet.
Es wird versucht, 0 Patches zu downloaden.
Der Patchdownload wurde beendet.
Es wurden neue Informationen zur Patchquelle und/oder Sprache gefunden.
Nicht lizenzierter Inhalt wird entfernt.
Das Aktualisieren der Definitionen ist abgeschlossen.
Details ausblenden
Protokoll anzeigen...
Schließen

VORSICHT: Schließen Sie keinesfalls die Konsole während eines manuellen Updates
Schließen Sie keinesfalls die Konsole, während ein manueller Updateprozess für Sicherheitsinhalte ausgeführt wird, denn sonst wird der Prozess abgebrochen. Diese Regel gilt jedoch nicht für einen geplanten Task, dessen Verarbeitung abgeschlossen wird, selbst wenn die Konsole während des Vorgangs geschlossen wird.

So konfigurieren Sie den Speicherort für den Patchdownload

1. Klicken Sie im Dialogfeld **Updates downloaden** auf die Registerkarte **Patchspeicherort**.
2. Geben Sie einen UNC-Pfad für die kopierten Patchdateien an. Der Standardspeicherort ist das Verzeichnis \LDLogon\Patch des Coreservers.
3. Wenn der oben eingegebene UNC-Pfad auf einen anderen Speicherort als den Coreserver zeigt, geben Sie einen gültigen Benutzernamen und ein Kennwort ein, um sich bei diesem Speicherort zu authentifizieren.
4. Geben Sie eine URL ein, über die Geräte auf die heruntergeladenen Patches für die Verteilung zugreifen können. Diese URL sollte dem oben angegebenen UNC-Pfad entsprechen.
5. Sie können auf **Testeinstellungen** klicken, um zu prüfen, ob mit der oben angegebenen Webadresse eine Verbindung hergestellt werden kann.
6. Wenn Sie den UNC-Pfad und die URL-Adresse wieder auf die Standardeinstellungen für den Speicherort zurücksetzen möchten, klicken Sie auf **Standardeinstellungen wiederherstellen**. Wiederum ist der Standardspeicherort das Verzeichnis \LDLogon\Patch des Coreservers.

Planen von automatischen Updates für Sicherheitsinhalte

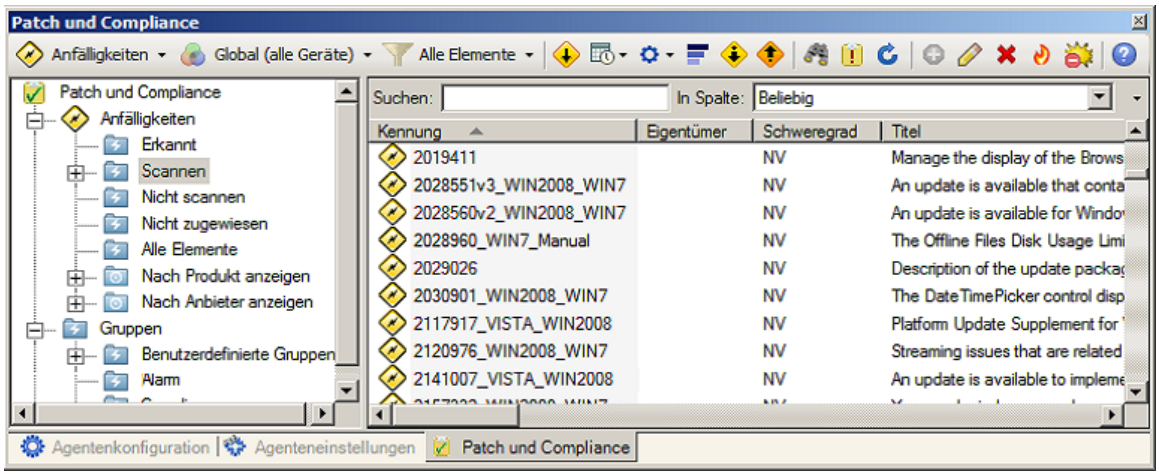
Sie können Updates für Sicherheitsinhalte auch als geplanten Task konfigurieren, der zu einem festgelegten Zeitpunkt oder als wiederkehrender Task ausgeführt wird. Klicken Sie hierfür ganz einfach in der Symbolleiste auf die Schaltfläche **Download planen**. Das Dialogfeld **Informationen zum geplanten Update** zeigt taskspezifische Einstellungen für den Task an. Klicken Sie auf **OK**, um einen Task der Kategorie "Sicherheitsinhalte downloaden" im Fenster "Geplante Tasks", in dem Sie die Zeitplanoptionen festlegen können, zu erstellen.

WICHTIG: Taskspezifische Einstellungen und globale Einstellungen
Beachten Sie, dass nur die Definitionstyp-, Sprach- sowie Definitions- und Patch-Downloadeinstellungen gespeichert und mit einem spezifischen Task während dessen Erstellung verknüpft werden. Diese drei Einstellungen gelten als taskspezifisch. Alle anderen Einstellungen auf den anderen Seiten des Dialogfeldes **Updates downloaden** sind global, d. h., sie gelten für alle nachfolgenden Downloadtasks für Sicherheitsinhalte. Die globalen Einstellungen umfassen: Patchdownload-Speicherort, Proxyserver, Spyware-Autofix, Sicherheitsalarme und Antivirus. Jedes Mal, wenn Sie globale Einstellungen ändern, gilt diese Änderung für alle Sicherheitsinhalt-Downloadtasks von diesem Punkt an.

Anzeigen und Ordnen von Sicherheitsinhalten

Nachdem der Sicherheitsinhalt aktualisiert wurde, können Sie die Definitionen und Erkennungsregeln (für Anfälligkeiten und benutzerdefinierte Definitionen) nur in ihren entsprechenden Gruppen im Fenster des Extras "Patch und Compliance" anzeigen.

Verwenden Sie die Dropdownliste **Typ**, um den Inhalt für einen bestimmten Definitionstyp oder für alle Definitionstypen anzuzeigen. Mit dem Steuerelement **Filter** können Sie den Inhalt, den Sie anzeigen möchten, zusätzlich anpassen.



Nachdem der Sicherheitsinhalt heruntergeladen wurde, können Sie Elemente in andere Statusgruppen verschieben oder in Ihre eigene benutzerdefinierte Gruppe kopieren. Informationen dazu, wie die verschiedenen Gruppen verwendet werden, finden Sie unter "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584.

Sie können die Eigenschaften der einzelnen aktualisierten Definitionen und Erkennungsregeln betrachten, indem Sie mit der rechten Maustaste auf ein Element klicken und **Eigenschaften** auswählen. Anhand dieser Informationen können Sie bestimmen, welche Definitionen für die von Ihrem Netzwerk unterstützten Plattformen und Anwendungen von Belang sind, wie Erkennungsregeln Definitionen aufspüren, welche Patches verfügbar sind und wie Sie Reparaturmaßnahmen für die betroffenen Geräte konfigurieren und ausführen sollten.

HINWEIS: Benutzerdefinierte Definitionen können bearbeitet werden
Wenn Sie eine heruntergeladene Definition auswählen, die von einem Anbieter der IT-Branche veröffentlicht wurde, dient das Dialogfeld in dem die Eigenschaften dieser Definition angezeigt werden, in erster Linie der Information. Wählen Sie hingegen eine benutzerdefinierte Definition aus oder erstellen eine neue benutzerdefinierte Definition, so sind die Felder im Dialogfeld "Eigenschaften" editierbar. Dadurch erhalten Sie die Möglichkeit, die Definition und ihre Erkennungsregeln zu definieren.

Suchen nach Anfälligkeiten anhand des CVE-Namens

Patch und Compliance unterstützt den Benennungsstandard nach CVE (Common Vulnerabilities and Exposures). Sie können mit dem CVE-Namen nach einer heruntergeladenen Anfälligkeit suchen. Sie können außerdem den/die mit einer bestimmten Anfälligkeit verknüpften CVE-Namen anzeigen.

Was ist CVE?

CVE ist die Abkürzung für "Common Vulnerabilities and Exposures" – eine von mehreren führenden Organisationen der Sicherheitsbranche gemeinsam geleitete Initiative, die darauf abzielt, eine Liste standardisierter Namen für Anfälligkeiten und andere Sicherheitsbedrohungen zu erfassen und zu verwalten. CVE ist keine Datenbank, sondern vielmehr ein Wörterbuch mit Namenseinträgen.

Das erklärte Ziel des CVE-Benennungsstandards besteht im Wesentlichen darin, die Suche, den Zugriff und die gemeinsame Nutzung von Daten über mehrere Anfälligkeitsdatenbanken und Sicherheitstools hinweg zu vereinfachen. Ausführliche Informationen zu CVE und dem CVE Editorial Board finden Sie auf der Website der MITRE Corporation.

LANDesk Kompatibilität mit dem CVE-Benennungsstandard

Die Produkte von LANDesk, einschließlich dem Kernprodukt LANDesk Management Suite sowie LANDesk Security Suite und LANDesk Patch Manager, bieten Tools für die Aktualisierung, Anzeige und Berichterstellung zu Anfälligkeitsdefinitionen, die den CVE-Standard uneingeschränkt unterstützen.

Wenn Sie Updates für Anfälligkeitsdefinitionen herunterladen, enthalten die Anfälligkeitsdaten CVE-Namensverweise, die auf den neuesten Informationen des CVE-Gremiums basieren. Zusätzlich enthält die Anfälligkeitsdefinition einen Hyperlink zur CVE-Wörterbuch-Website, auf der Sie die neuesten CVE-Versionsinformationen direkt von der Quelle beziehen können. Die Genauigkeit und Aktualität der CVE-Daten wird durch diesen direkten Link gewährleistet.

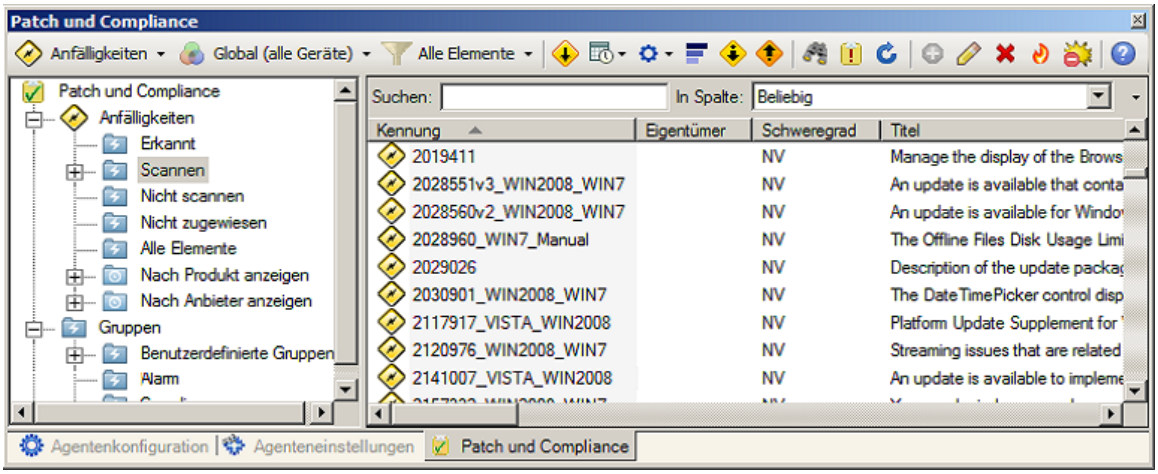
Suchen nach Anfälligkeiten anhand ihres CVE-Namens

Patch und Compliance bietet Ihnen die Möglichkeit, die Suche nach Anfälligkeiten anhand der eindeutigen CVE-Namen der Anfälligkeiten durchzuführen.

Sie können auch CVE-Namen für heruntergeladene Anfälligkeiten suchen und die CVE-Website öffnen, um weitere Informationen über die Anfälligkeit und ihren CVE-Status zu erhalten.

So suchen Sie nach Anfälligkeitsdefinitionen anhand des CVE-Namens

1. Wählen Sie im Extra-Fenster **Patch und Compliance** die Option **Anfälligkeiten** aus der Dropdownliste **Typ** aus. Eine vollständige Liste heruntergeladener Anfälligkeitsdefinitionen wird angezeigt.



2. Geben Sie den CVE-Namen (die CVE-Kennung) in das Feld **Suchen** ein, wählen Sie in der Liste **In Spalte** die Option **Jede** oder **CVE-Kennung** aus und klicken Sie dann auf die Schaltfläche **Suchen**. (Sie können die gesamte CVE-Kennung (einschließlich cve-Präfix) oder nur den Ihnen bekannten Teil der Kennung eingeben und Ihr heruntergeladenes Sicherheitsrepository auf Anfälligkeiten durchsuchen, die den Suchkriterien entsprechen.)
3. Wenn eine Anfälligkeit mit einer übereinstimmenden CVE-Kennung in dem von Ihnen heruntergeladenen Anfälligkeitenrepository gefunden wird, wird sie in der Liste angezeigt.
4. Klicken Sie mit der rechten Maustaste auf die Anfälligkeit, um auf ihr Kontextmenü und die darin enthaltenen Optionen zuzugreifen.

So suchen Sie nach CVE-Namen für heruntergeladene Anfälligkeitsdefinitionen

1. Wählen Sie in **Patch und Compliance** in der Liste **Typ** die Option **Anfälligkeiten** oder **Alle Typen** aus. Eine Liste heruntergeladener Definitionen wird angezeigt. (Wenn die Spalte für CVE-Kennungsdaten ausgewählt wurde, können Sie CVE-Kennungen in der Elementliste anzeigen. Um Spalten zu konfigurieren, klicken Sie mit der rechten Maustaste auf die Titelleiste einer Spalte, wählen Sie **Spalten** aus und stellen Sie sicher, dass die Spalte **CVE-Kennung** in der Liste **Ausgewählte Spalten** enthalten ist.)
2. Doppelklicken Sie auf eine Anfälligkeitsdefinition (oder klicken Sie mit der rechten Maustaste auf die Definition und wählen Sie **Eigenschaften** aus), um das Dialogfeld **Eigenschaften** der Anfälligkeit zu öffnen.
3. Klicken Sie auf die Seite **Beschreibung**.
4. Wenn die ausgewählte Anfälligkeit über einen CVE-Namen verfügt, wird dieser in der Liste **CVE-Kennung** angezeigt. Einige Anfälligkeiten verfügen möglicherweise über mehrere CVE-Namen, auf die Sie mit einem Bildlauf in der Liste zugreifen können.
5. Um die Webseite für eine bestimmte CVE-Kennung zu öffnen, klicken Sie auf den Link **Weitere Informationen für CVE-Kennung**. Die CVE-Website enthält detaillierte Informationen zu jeder Anfälligkeit, die über einen CVE-Namen verfügt, einschließlich des aktuellen Status der Anfälligkeit im CVE-Gremium (genehmigter oder nicht genehmigter Eintrag).

Anpassen von Elementlisten mit Filtern

Mit der Liste **Filter** können Sie benutzerdefinierte Anzeigefilter erstellen und aktivieren, um auf diese Weise zu steuern, welche Elemente im rechten Fensterausschnitt des Extras angezeigt werden. Filter können dazu beitragen, große Mengen an Sicherheitsinhalt übersichtlicher zu organisieren. Sie können Inhalte nach Betriebssystem und Schweregrad filtern.

Das Steuerungselement **Filter** kann zusammen mit dem Steuerungselement **Typ** dazu verwendet werden, genau den Sicherheitsinhalt anzuzeigen, den Sie ansehen möchten.

So erstellen Sie einen neuen Anzeigefilter

1. Klicken Sie in Patch und Compliance auf die Dropdownliste **Filter** und dann auf **Filter verwalten**.
2. Klicken Sie auf **Neu**.
3. Geben Sie einen Namen für den neuen Filter ein.
4. Wenn Sie den Inhalt nach Betriebssystem filtern möchten, aktivieren Sie das Kontrollkästchen **Betriebssystem** und wählen dann das Betriebssystem aus, das Sie anzeigen möchten.
5. Wenn Sie den Inhalt nach dem Schweregrad der Definition filtern möchten, aktivieren Sie das Kontrollkästchen **Schweregrad** und wählen dann die Schweregrade aus, die Sie anzeigen möchten. Klicken Sie auf **OK**.

So wenden Sie eine Filter auf die Anzeige einer Inhaltsgruppe an

1. Klicken Sie auf die Inhaltsgruppe im linken Fensterausschnitt.
2. Klicken Sie auf die Dropdownliste **Filter** und wählen Sie dann einen Filter aus der Liste aus.

Löschen von nicht verwendeten Sicherheitsinhaltsdefinitionen

Sie können nicht verwendete Definitionen dauerhaft aus dem Fenster des Extras "Patch und Compliance" (und der Coredatenbank) löschen, wenn Sie feststellen, dass diese Informationen für Ihre Umgebung nicht von Belang oder nach einem erfolgreichen Reparaturvorgang veraltet sind.

Beim Tilgen von Definitionen werden auch die zugehörigen Erkennungsregeldaten aus den Erkennungsregelgruppen in der Strukturansicht entfernt. Die eigentlichen verknüpften ausführbaren Patchdateien werden bei diesem Vorgang jedoch nicht entfernt. Die Patchdateien müssen manuell aus der lokalen Ablage gelöscht werden, die sich in der Regel auf dem Coreserver befindet.

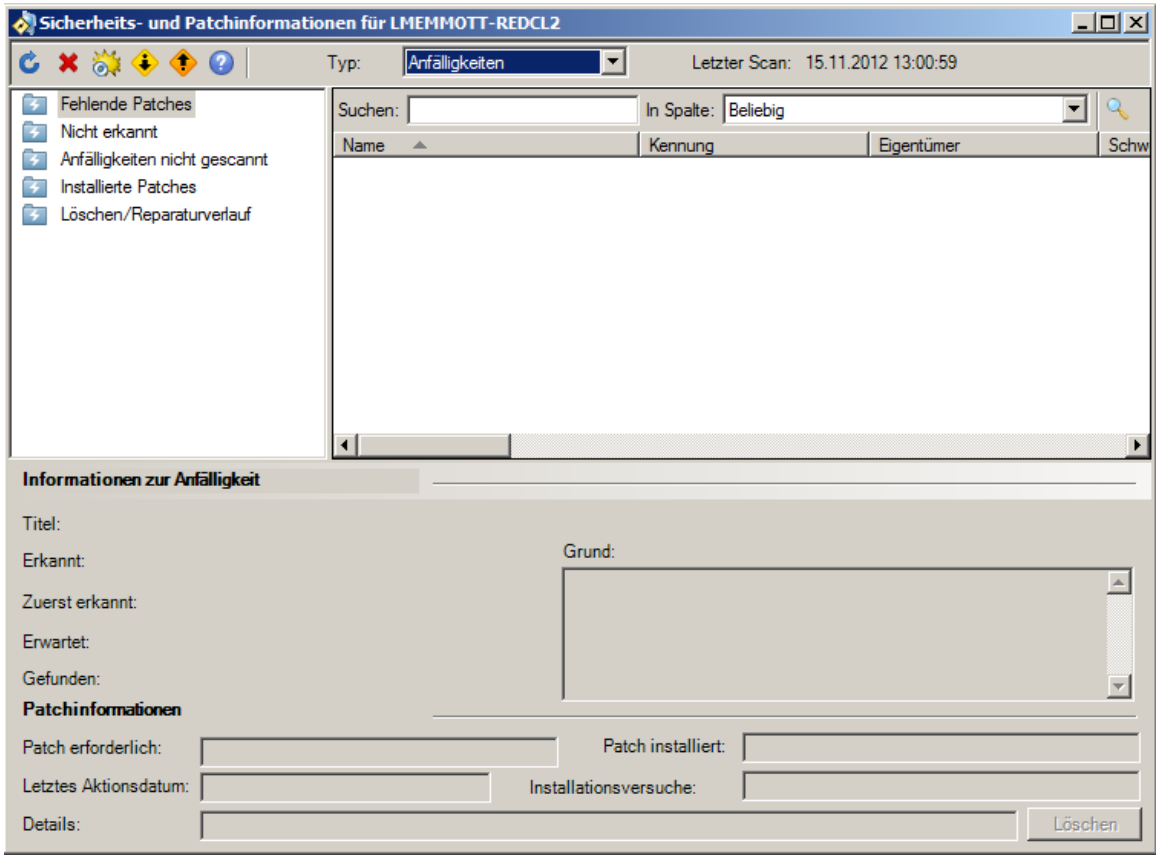
So tilgen Sie nicht verwendete Definitionen

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie auf die Schaltfläche **Nicht verwendete Definitionen löschen** in der Symbolleiste.
3. Wählen Sie die Plattformen aus, deren Definitionen Sie entfernen möchten. Sie können eine oder mehrere Plattformen aus der Liste wählen. Falls eine Definition mit mehreren Plattformen verbunden ist, müssen Sie alle mit der Definition verknüpften Plattformen auswählen, damit die Definition entfernt wird.
4. Wählen Sie die Sprachen aus, deren Definition Sie entfernen möchten (verknüpft mit der oben ausgewählten Plattform). Wenn Sie oben eine Windows- oder Macintosh-Plattform auswählen, sollten Sie die Sprachen angeben, deren Definition Sie entfernen möchten. Wenn Sie oben eine UNIX- oder Linux-Plattform ausgewählt haben, müssen Sie die Option "Sprache neutral" auswählen, damit ihre sprachübergreifenden Definitionen entfernt werden.
5. Klicken Sie auf **Entfernen**.

Anzeigen von Sicherheitsinformationen für ein gescanntes Gerät

Sie können auch auf gescannte Geräte bezogene Informationen direkt in der Netzwerkansicht anzeigen, indem Sie auf eines oder mehrere der ausgewählten Geräte mit der rechten Maustaste klicken und dann auf **Sicherheits- und Patchinformationen** klicken.

In diesem Dialogfeld können Sie Informationen zum Verlauf der Erkennung, Installation und Reparatur anzeigen und Patchverwaltungstasks ausführen.



Herunterladen von Patches

Damit Sicherheitspatches an betroffene Geräte verteilt werden können, *muss* die ausführbare Datei des Patches auf ein lokales Patchrepository im lokalen Netzwerk gedownloadet werden. Als Standardspeicherort für Patchdateidownloads ist das folgende Verzeichnis auf dem Coreserver:

/LDLogon/Patches

Sie können diesen Speicherort auf der Registerkarte "Patchspeicherort" des Dialogfelds "Updates downloaden" ändern.

Sie können jedes Patch einzeln oder mehrere Patches gleichzeitig downloaden.

HINWEIS: Speicherort für Patchdownloads und Proxyservereinstellungen
Bei Patchdownloads werden immer die aktuellen Einstellungen für den Downloadspeicherort aus der Registerkarte "Patchspeicherort" des Dialogfelds "Updates downloaden" verwendet. Falls Ihr Netzwerk einen Proxyserver für den Internetzugang verwendet, müssen Sie außerdem daran denken, zuerst die Einstellungen des Proxyservers auf der Seite "Proxyeinstellungen" zu konfigurieren, da Sie andernfalls keine Patchdateien downloaden können.

Patch und Compliance versucht zuerst, Patchdateien von der im Dialogfeld "Patcheigenschaften" angezeigten URL herunterzuladen. Falls keine Verbindung hergestellt werden kann oder das Patch nicht verfügbar ist, wird das Patch vom LANDesk-Sicherheitsdienst heruntergeladen; hierbei handelt es sich um eine von LANDesk bereitgestellte Datenbank, die Patches aus vertrauenswürdigen Quellen der IT-Branche enthält.

Downloadverfahren

Verwenden Sie eines der folgenden Verfahren zum Downloaden von Patches:

- Über das Dialogfeld "Updates downloaden"
- Über eine Erkennungsregel
- Über eine Sicherheitsdefinition

Über das Dialogfeld "Updates downloaden" können Sie Patches und gleichzeitig die zugehörigen Sicherheitsdefinitionen downloaden.

Sie können Patches auch direkt über eine Erkennungsregel oder eine Sicherheitsdefinition downloaden.

So downloaden Sie Patches über eine Erkennungsregel

1. Klicken Sie von einer beliebigen Gruppe mit **Erkennungsregeln** mit der rechten Maustaste auf eine Erkennungsregel und klicken Sie dann auf **Patches downloaden**. (Sie können auch Patches für benutzerdefinierte Definitionen aus dem Dialogfeld "Erkennungsregel" downloaden, wenn Sie eine benutzerdefinierte Definition erstellen oder bearbeiten.)
2. Um eine Gruppe von Patches herunterzuladen, wählen Sie eine beliebige Anzahl von Regeln in einer der Gruppen mit **Erkennungsregeln** aus, klicken mit der rechten Maustaste auf die Auswahl und klicken dann auf **Patches downloaden**.
3. Informationen zum Downloadvorgang und -status werden im Dialogfeld **Patches werden gedownloadet** angezeigt. Sie können jederzeit auf **Abbrechen** klicken, um den gesamten Downloadvorgang zu stoppen.
4. Wenn der Download beendet ist, klicken Sie auf die Schaltfläche **Schließen**.

HINWEIS: Mit einer Erkennungsregel können Sie Patches auch über das zugehörige Dialogfeld "Eigenschaften" downloaden (**Eigenschaften > Patchinformationen > Download**).

So downloaden Sie verknüpfte Patches über eine Sicherheitsdefinition

1. Klicken Sie mit der rechten Maustaste auf die Sicherheitsdefinition und klicken Sie dann auf **Verknüpfte Patches downloaden**.
2. Wählen Sie, ob Sie alle verknüpften Patches oder nur aktuelle Patches downloaden wollen.
3. Klicken Sie auf **Downloaden**.

Weitere Informationen zum Downloadstatus von Patchdateien finden Sie unter "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584.

Deinstallieren von Patches (Patch-Rollback)

Patches, die an verwaltete Geräte verteilt wurden, können (per Rollback) deinstalliert werden. Beispiel: Sie möchten ein Patch deinstallieren, das einen unerwarteten Konflikt mit einer vorhandenen Konfiguration verursacht. Indem Sie das Patch deinstallieren, können Sie den ursprünglichen Zustand des Geräts wiederherstellen.

So deinstallieren Sie ein Patch bzw. führen ein Patch-Rollback durch

1. Klicken Sie in einer beliebigen Liste mit Erkennungsregeln mit der rechten Maustaste auf mindestens eine Erkennungsregel und klicken Sie dann auf **Patch deinstallieren**.
2. Geben Sie einen Namen für den Deinstallationstask ein.
3. Geben Sie an, ober die Deinstallation ein geplanter Task, ein richtlinienbasierter Scan oder beides ist.
4. Wenn Sie "geplante Aufgabe" ausgewählt haben, geben Sie an, auf welchen Geräten Sie das Patch deinstallieren möchten.
5. Wenn sich das Patch ohne Zugriff auf seine ursprüngliche ausführbare Datei nicht deinstallieren lässt (d. h. unter Verwendung von Befehlszeilenparametern) und Sie die ausführbare Datei mittels Targeted Multicast verteilen möchten, aktivieren Sie das Kontrollkästchen **Multicast verwenden**. Zum Konfigurieren der Multicast-Optionen klicken Sie auf die Schaltfläche **Multicast-Optionen**. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "Multicastoptionen"" auf Seite 674.
6. Wenn Sie "Richtlinie" ausgewählt haben und Sie auf der Basis dieses Deinstallationstasks eine neue Abfrage erstellen möchten, die sich später wieder verwenden lässt, aktivieren Sie das Kontrollkästchen **Abfrage hinzufügen**.
7. Wählen Sie Scan- und Reparatureinstellungen aus der Liste der verfügbaren Einstellungen aus (oder erstellen Sie benutzerdefinierte Einstellungen für diesen Scan), um festzulegen, wie der Scan auf Endbenutzergeräten ausgeführt wird.
8. Klicken Sie auf **OK**. Für einen geplanten Task können Sie jetzt Zielgeräte hinzufügen und die Zeitplanoptionen im Extra "Geplante Tasks" konfigurieren. Für eine Richtlinie wird die neue Richtlinie im Application Policy Management-Fenster unter dem oben angegebenen Task-Namen angezeigt. Hier können Sie jetzt statische Ziele (Benutzer oder Geräte) und dynamische Ziele (Abfrageergebnisse) hinzufügen sowie Typ und Häufigkeit der Richtlinie konfigurieren.

Falls die Patchinstallation misslungen ist, müssen Sie zuerst die den Installationsstatus betreffenden Informationen löschen, bevor Sie erneut versuchen, das Patch zu installieren. Sie können die Installations-/Reparaturstatusinformationen für das betroffene Gerät löschen, indem Sie im Dialogfeld **Sicherheits- und Patchinformationen** auf **Löschen** klicken. Sie können außerdem den Patchinstallationsstatus nach Anfälligkeit löschen.

Patches aus der Coredatenbank entfernen

Um Patchdateien dauerhaft zu entfernen, müssen Sie die Dateien aus dem Patchrepository löschen, das sich für gewöhnlich auf dem Coreserver befindet.

Rechtshinweis zum Typ "Blockierte Anwendung"

WICHTIG: Als Service für seine Endanwender bietet LANDesk Zugriff auf eine Datenbank mit speziellen Informationen zu ausführbaren Dateien, die u. U. von einem Endanwender im Zusammenhang mit der Anwendungsblockerfunktion von LANDesk Security Suite verwendet werden. DIESE INFORMATIONEN WERDEN WIE BESEHEN UND OHNE JEGLICHE AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER SONSTIGE GEWÄHRLEISTUNG, EINSCHLIESSLICH KONKLUDENTER GEWÄHRLEISTUNGEN HINSICHTLICH HANDELSÜBLICHKEIT UND/ODER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, ZUR VERFÜGUNG GESTELLT. LANDesk übernimmt keine Garantie hinsichtlich der Genauigkeit, Vollständigkeit oder Aktualität dieser Informationen. Es ist Aufgabe des Endanwenders, sich vor Verwendung der Informationen von der Richtigkeit dieser Informationen zu überzeugen. Die Verwendung dieser Informationen erfolgt ausschließlich auf eigenes Risiko des Endanwenders.

Manche der Übersichtsinformationen in den Definitionen von blockierten Anwendungen werden von http://www.sysinfo.org bereitgestellt und sind wie folgt urheberrechtlich geschützt: "Präsentation, Format und Kommentare Copyright © 2001 – 2005 Paul Collins; Portions Copyright © Peter Forrest, Denny Denham, Sylvain Prevost, Tony Klein; Datenbankerstellung und Support von Patrick Kolla; Softwaresupport von John Mayer. Alle Rechte vorbehalten."

Benutzerdefinierte Sicherheitsdefinitionen – Übersicht

Zusätzlich zu bekannten Anfälligkeiten, die Sie über das Extra "Patch und Compliance" aktualisieren, können Sie auch eigene benutzerdefinierte (oder angepasste) Definitionen erstellen – einschließlich benutzerdefinierter Erkennungsregeln, verknüpfter Patchdateien und spezieller Zusatzbefehle, die eine erfolgreiche Reparatur gewährleisten.

Anfälligkeitsdefinitionen bestehen aus einer eindeutigen Kennung, Titel, Datum der Veröffentlichung, Sprache, zusätzlichen Identifizierungsdaten und den Erkennungsregeln, die dem Sicherheitsscanner mitteilen, wonach er auf Zielgeräten suchen soll. Erkennungsregeln definieren die Plattform, Anwendung, Datei oder die Registrierungsbedingungen, nach der/denen der Sicherheitsscanner sucht, um eine Anfälligkeit (oder praktisch *jede* beliebige Systembedingung bzw. *jeden* beliebigen Systemstatus) auf gescannten Geräten ausfindig zu machen.

Die benutzerdefinierten Anfälligkeitsdefinitionen sind eine leistungsstarke, flexible Funktion, mit der Sie eine zusätzliche systembezogene Ebene der Patchsicherheit auf Ihrem LANDesk System realisieren können. Zusätzlich zur Verbesserung der Patchsicherheit und anderen innovativen Tasks, die die Vorteile der Scanfunktionen des Anfälligkeitsscanners nutzen, können benutzerdefinierte Anfälligkeiten u.a. auch dazu verwendet werden, Systemkonfigurationen zu analysieren, nach bestimmten Datei- und Registrierungseinstellungen zu suchen und Anwendungsaktualisierungen zu verteilen.

HINWEIS: Erstellen benutzerdefinierter Definitionen für blockierte Anwendungen
Sie können eigene benutzerdefinierte Definitionen für den Anwendungstyp "Blockierte Anwendung" erstellen. Wählen Sie in der Dropdownliste **Typ** die Option **Blockierte Anwendungen**, geben Sie den Namen einer ausführbaren Datei und einen beschreibenden Titel für die Bezeichnung ein und klicken Sie dann auf **OK**.

Benutzerdefinierte Definitionen müssen nicht notwendigerweise Reparaturaktionen (Verteilen und Installieren von Patchdateien) ausführen. Wenn die benutzerdefinierte Definition mit einer "Nur erkennen"-Erkennungsregel oder mit Regeln definiert wurde, die nur von Patch und Compliance erkannt werden können, tastet der Sicherheitsscanner die Zielgeräte ab und meldet, auf welchen Geräten die vorgeschriebene Bedingung (Anfälligkeit) gefunden wurde. Sie können beispielsweise eine nur auf die Erkennung begrenzte benutzerdefinierte Regel für den Sicherheitsscanner schreiben, mit der verwaltete Geräte auf Folgendes geprüft werden können:

- Anwendung: %s
- Datei: %s
- Dateiversion
- Paketspeicherort:
- Dateidatum
- Registrierungseinstellung

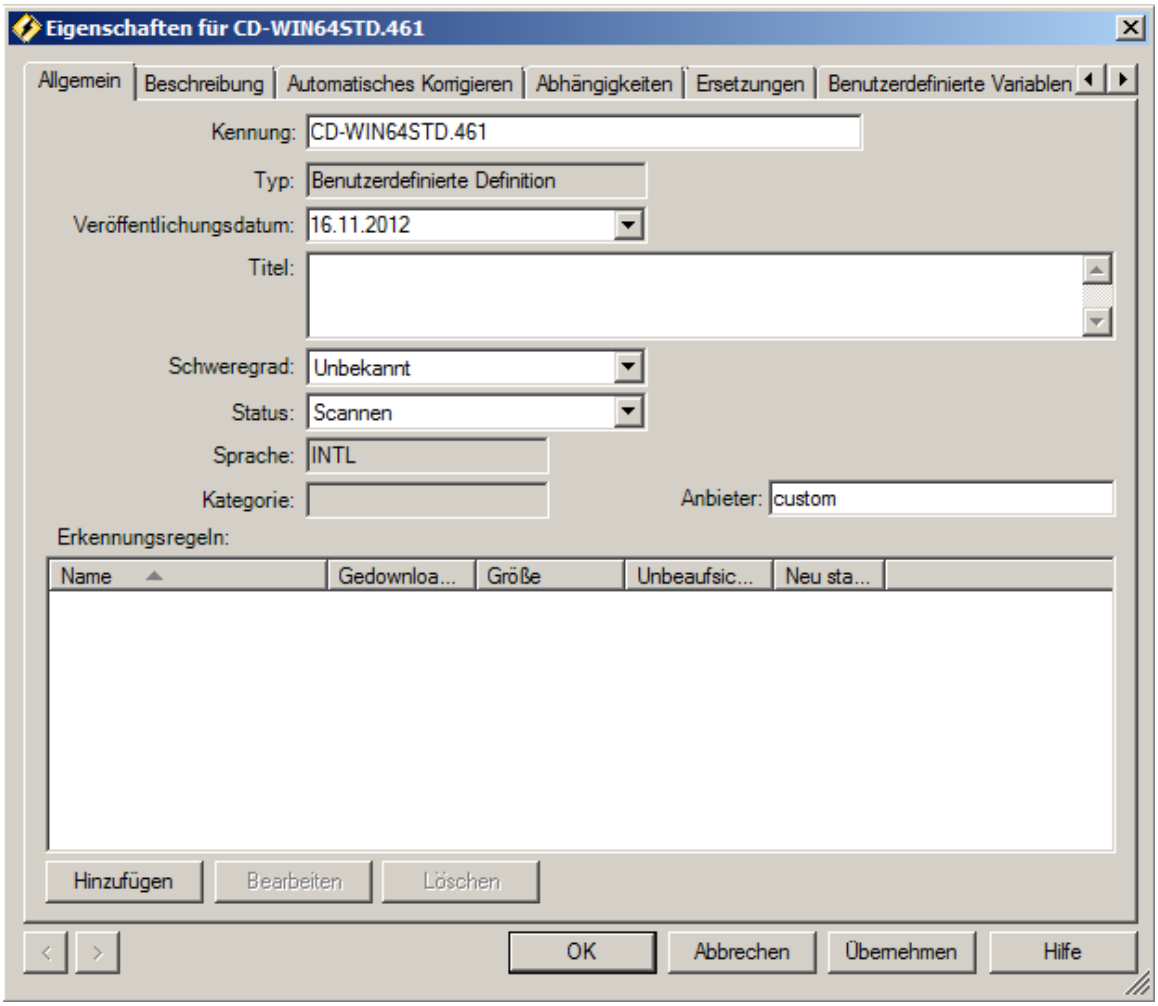
Sie können so viele benutzerdefinierte Definitionen erstellen, wie Sie für das Einrichten und Aufrechterhalten einer optimalen Stufe der Patchsicherheit in Ihrer Umgebung benötigen.

Erstellen von benutzerdefinierten Sicherheitsdefinitionen

So erstellen Sie benutzerdefinierte Definitionen

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Wählen Sie in der Liste **Typ** die Option **Alle Typen** oder **Benutzerdefinierte Definitionen** aus. (Die Symbolleistenschaltfläche **Benutzerdefinierte Definition erstellen** steht nur zur Verfügung, wenn einer dieser beiden Typen ausgewählt wurde; oder wenn der Typ **Blockierte Anwendungen** ausgewählt wurde, falls Sie eine benutzerdefinierte Definition für eine zu blockierende Anwendung erstellen möchten.)

3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Benutzerdefinierte Definition erstellen**. Es wird eine editierbare Version des Dialogfelds "Eigenschaften" geöffnet. In diesem Dialogfeld können Sie nach Bedarf Anfälligkeitseinstellungen konfigurieren.



4. Geben Sie eine eindeutige Kennung für die Anfälligkeit ein. (Der vom System generierte Erkennungscode kann bearbeitet werden.)
5. Dieser Typ ist eine "Benutzerdefinierte Definition" und kann nicht geändert werden.
6. Das Datum der Veröffentlichung ist das aktuelle Datum und kann nicht geändert werden.
7. Geben Sie einen beschreibenden Titel für die Anfälligkeit ein. Dieser Titel wird in der Anfälligkeitsliste angezeigt.
8. Geben Sie den Schweregrad an. Zu den verfügbaren Optionen gehören: Unbekannt, Service Pack, Kritisch, Hoch, Mittel, Niedrig und Nicht anwendbar.
9. Geben Sie den Status der Anfälligkeit ein. Zu den verfügbaren Optionen gehören: "Nicht scannen", "Scannen" und "Nicht zugewiesen". Wenn Sie einen Status angeben, wird die Anfälligkeit in die entsprechende Gruppe in der Strukturansicht aufgenommen (siehe "Strukturansicht" auf Seite 588).

10. Die Spracheinstellungen für benutzerdefinierte Anfälligkeiten sind automatisch auf INTL (international oder sprachneutral) gesetzt. Dies bedeutet, dass die Anfälligkeit auf jede Sprachversion des Betriebssystems und/oder der Anwendungen angewendet werden kann.
11. Die Liste "Erkennungsregeln" zeigt alle Regeln an, die von dieser Anfälligkeit verwendet werden. Wenn Sie eine neue benutzerdefinierte Anfälligkeit erstellen, sollten Sie mindestens eine Erkennungsregel definieren, die vom Sicherheitsscanner für das Scannen nach dieser Anfälligkeit eingesetzt wird. Klicken Sie auf **Hinzufügen**, um Erkennungsregeln hinzuzufügen. (Lesen Sie hierzu die Anleitungen weiter unten).
12. Wenn Sie zusätzliche Informationen zu dieser Anfälligkeit bereitstellen möchten, klicken Sie auf **Beschreibung** und geben Ihre Kommentare in das Textfeld und/oder eine gültige Webadresse ein, auf der weitere Informationen zu finden sind.
13. Wenn Sie Voraussetzungen für diese benutzerdefinierte Anfälligkeitsdefinition definieren möchten (und andere Definitionen einsehen möchten, die von dieser Anfälligkeit abhängig sind), klicken Sie auf **Abhängigkeiten** und konfigurieren die Definitionen für die Voraussetzungen.
14. Wenn Sie Ihre eigenen benutzerdefinierten Variablen für diese benutzerdefinierte Anfälligkeitsdefinition erstellen (oder bearbeiten) möchten, klicken Sie auf **Benutzerdefinierte Variablen** und konfigurieren die benutzerdefinierten Variablen.
15. Wenn Sie die Definition der Attribute für die benutzerdefinierte Variable abgeschlossen haben, klicken Sie auf **OK**, um das Dialogfeld zu schließen und die Anfälligkeitsdefinition zu speichern.

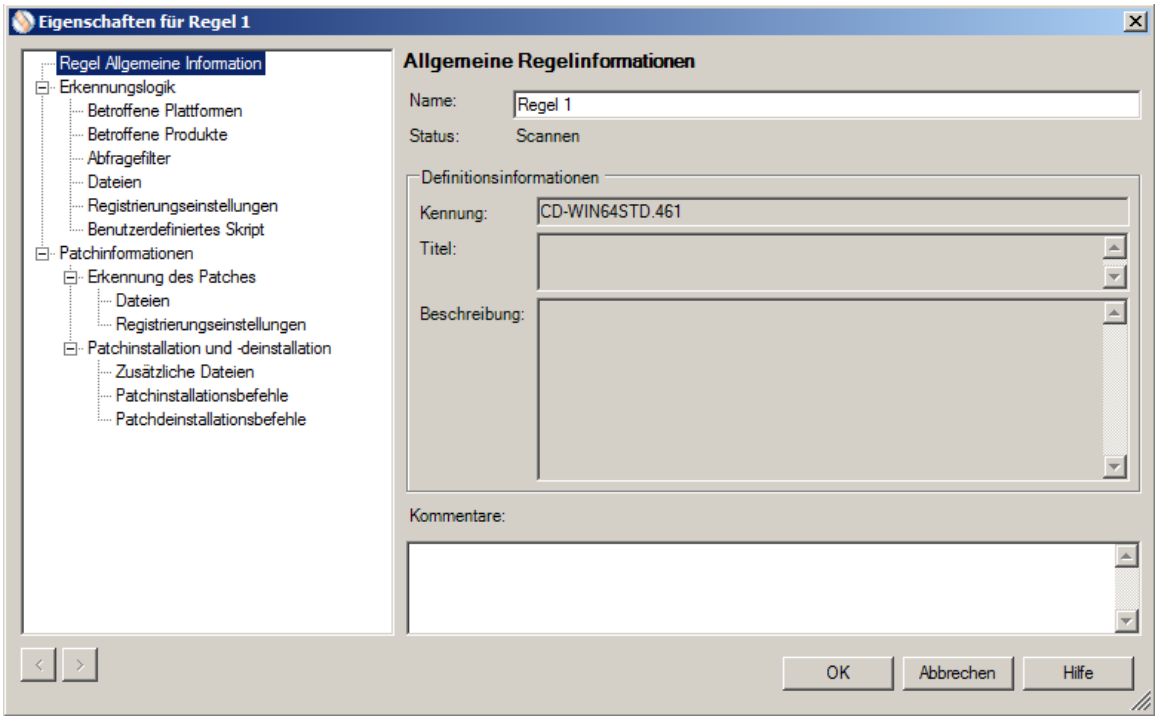
Wie bei den bekannten Anfälligkeiten der Anbieter sollten auch benutzerdefinierte Anfälligkeiten eine oder mehrere Erkennungsregeln beinhalten, die dem Sicherheitsscanner mitteilen, nach welchen Bedingungen beim Scannen verwalteter Geräte gesucht werden sollte. Führen Sie die nachstehend beschriebenen Schritte aus, um eine Erkennungsregel für eine benutzerdefinierte Anfälligkeit zu erstellen.

Erstellen von benutzerdefinierten Erkennungsregeln

So erstellen Sie benutzerdefinierte Erkennungsregeln

1. Klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Definition und klicken Sie dann auf **Eigenschaften**. (Oder doppelklicken Sie auf die Anfälligkeitsdefinition.)

2. Klicken Sie auf die Schaltfläche **Hinzufügen**, die sich unter der Liste "Erkennungsregeln" befindet. Eine editierbare Version des Dialogfelds "Regeleigenschaften" wird auf der Seite "Allgemeine Informationen" des Dialogfelds geöffnet und gibt Ihnen die Möglichkeit, eine Erkennungsregel zu konfigurieren.



3. Geben Sie auf der Seite "Allgemeine Informationen" einen eindeutigen Namen für die Regel ein. Der Regelstatus lässt sich hier nicht bearbeiten. Um den Status einer Erkennungsregel zu ändern, klicken Sie in einer der Listenansichten mit der rechten Maustaste auf die Regel. Klicken Sie dann, je nach aktuellem Status, auf **Aktivieren** oder **Deaktivieren**. Die Definitionsinformationen der Regel lassen sich hier nicht bearbeiten. Sie können jedoch jede beliebige Information in das Feld "Kommentare" eingeben.
4. Verwenden Sie die verschiedenen Seiten des Dialogfelds "Regeleigenschaften", um die Erkennungsregel (wie im restlichen Abschnitt dieser Prozedur beschrieben) zu erstellen.
5. Öffnen Sie die "Erkennungslogik"-Seiten.
6. Wählen Sie auf der Seite "Betroffene Plattformen" die Plattformen aus, auf denen der Sicherheitsscanner nach der Definition dieser Erkennungsregeln suchen soll. Welche Plattformen als verfügbar in der Liste angezeigt werden, hängt davon ab, welche Anfälligkeiten Sie mithilfe des Extras "Patch und Compliance" aktualisiert haben. Klicken Sie auf **Standardplattformliste laden**, um die verfügbaren Plattformen zur Liste hinzuzufügen. Sie müssen mindestens eine Plattform auswählen.

7. Verknüpfen Sie die Regel auf der Seite "Betroffene Produkte" mit einer oder mehreren Softwareanwendungen. Klicken Sie zuerst auf **Bearbeiten**, um das Dialogfeld "Betroffene Produkte auswählen" zu öffnen. In diesem Dialogfeld können Sie Produkte zur Liste "Betroffene Produkte" hinzufügen oder daraus löschen (diese Liste lässt sich kürzen, indem Sie das Kontrollkästchen am unteren Rand des Dialogfelds aktivieren). Welche Produkte als verfügbar in der Liste angezeigt werden, hängt davon ab, welche Inhalte Sie aktualisiert haben. Sie müssen nicht unbedingt ein Produkt mit einer Erkennungsregel verknüpfen. Verknüpfte Produkte fungieren als Filter während des Sicherheitsscans. Wenn das angegebene verknüpfte Produkt auf dem Gerät gefunden wird, wird der Scan beendet. Wird das Produkt jedoch gefunden oder wurden keine Produkte angegeben, so setzt der Scanner die Dateiprüfung fort.
8. Konfigurieren Sie auf der Seite "Dateien" spezifische Dateibedingungen, nach der die Regel scannen soll. Klicken Sie auf **Hinzufügen**, um die Felder auf dieser Seite editierbar zu machen. Der erste Schritt beim Konfigurieren einer Dateibedingung ist das Festlegen der Überprüfungsmethode. Die ausgewählte Überprüfungsmethode bestimmt, welche Felder auf dieser Seite angezeigt werden. Zum Speichern einer Dateibedingung klicken Sie auf **Aktualisieren**. Sie können so viele Dateibedingungen hinzufügen, wie Sie möchten. Eine ausführliche Beschreibung dieser Option finden Sie unter "Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Dateien"" auf Seite 664.
9. Konfigurieren Sie auf der Seite "Registrierungseinstellungen" spezifische Registrierungsbedingungen, nach denen die Regel scannen soll. Klicken Sie auf **Hinzufügen**, um die Felder editierbar zu machen. Zum Speichern einer Registrierungsbedingung klicken Sie auf **Aktualisieren**. Sie können so viele Registrierungsbedingungen hinzufügen, wie Sie möchten. Eine ausführliche Beschreibung dieser Option finden Sie unter "Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Registrierungseinstellungen"" auf Seite 665.
10. Auf der Seite "Benutzerdefiniertes Skript" können Sie ein benutzerdefiniertes Visual Basic-Skript erstellen, das Sie beim Scannen mithilfe dieser Erkennungsregel unterstützt. Die Runtime-Eigenschaften des Sicherheitsscanners, auf die zum Abrufen von Ergebnisberichten mit einem benutzerdefinierten Skript zugegriffen werden kann, lauten: "Erkannt", "Grund", "Erwartet" und "Gefunden".

    HINWEIS: Sie können auf die Schaltfläche **Editor verwenden** klicken, um das mit diesem Dateityp assoziierte Standard-Skriptbearbeitungstool zu öffnen. Beim Schließen des Tools werden Sie aufgefordert, Ihre Änderungen auf der Seite "Benutzerdefiniertes Skript" zu speichern. Wenn Sie ein anderes Tool verwenden möchten, müssen Sie die Dateitypverknüpfung ändern.

11. Geben Sie auf der Seite "Patchinformationen" an, ob die mit dieser Erkennungsregel verknüpfte Anfälligkeit auf Ihren verwalteten Geräten repariert oder nur erkannt werden darf. Wenn Sie die Reparaturoption auswählen, werden die Felder "Patch Download Information" und "Reparaturdaten" editierbar.
12. Wenn sich die Reparatur durchführen lässt, indem Sie ein Patch verteilen, geben Sie den URL zu der betreffenden Patchdatei ein und geben Sie an, ob die Datei automatisch heruntergeladen werden kann. (Sie können versuchen, die verknüpfte Patchdatei herunterzuladen, indem Sie auf **Downloaden** klicken; oder Sie können die Datei zu einem späteren Zeitpunkt downloaden.)

13. Wenn sich die Reparatur mit einer Patchverteilung durchführen lässt, müssen Sie zudem einen eindeutigen Dateinamen für die Patchdatei eingeben und festlegen, ob nach der Patchverteilung ein Neustart durchgeführt werden muss, um den Reparaturvorgang komplett abzuschließen. Geben Sie auch an, ob das Patch während der Reparatur Eingaben seitens des Benutzers erforderlich macht. Im Falle einer Erkennungsregel, die das Reparieren von Anfälligkeiten einschließt, wird nachdrücklich empfohlen, ein Hash für die Patchdatei zu erstellen, indem Sie auf **MD5-Hash generieren** klicken. Die eigentliche Patchdatei muss heruntergeladen werden, damit Sie ein Hash erstellen können. Weitere Informationen zur Verwendung eines Hash finden Sie unter "Informationen zur Seite "Erkennungsregel: Allgemeine Informationen"" auf Seite 663.)
14. Für eine Regel, die das Reparieren der verknüpften Anfälligkeit einschließt, können Sie zusätzliche Befehle konfigurieren, die während der Reparatur auf den betroffenen Geräten ausgeführt werden. Um zusätzliche Reparaturbefehle zu konfigurieren, klicken Sie auf die Seite "Patchinstallationsbefehle" und klicken dann auf **Hinzufügen**, um einen Befehlstyp auszuwählen und die Argumentfelder des Befehls editierbar zu machen. Zusätzliche Patchinstallationsbefehle sind *nicht* erforderlich. Wenn Sie keine speziellen Befehle konfigurieren, wird die Patchdatei nur für sich ausgeführt, wie dies normalerweise der Fall ist. Eine ausführliche Beschreibung dieser Option finden Sie unter "Informationen zur Seite "Patchinstallationsbefehle"" auf Seite 668.

Nachdem Sie nun eine benutzerdefinierte Anfälligkeitsdefinition erstellt haben, können Sie diese Anfälligkeit genauso bearbeiten wie eine bekannte Anfälligkeit eines Herstellers oder Anbieters. Sie können den Status der Anfälligkeit auf "Scannen" setzen oder die Anfälligkeit zu der "Scannen"-Gruppe hinzufügen, die vom nächsten Sicherheitsscan erfasst werden soll. Sie können die Anfälligkeit zudem in die Gruppe "Nicht scannen" oder "Nicht zugewiesen" einfügen, betroffene Computer anzeigen, die Option "Automatisches Korrigieren" aktivieren, einen Reparaturauftrag erstellen oder den Scan-/Reparaturstatus löschen. Wählen Sie die betreffende Option aus, indem Sie durch Klicken mit der rechten Maustaste auf eine benutzerdefinierte Anfälligkeitsdefinition deren Kontextmenü öffnen.

Aktionen, die nur für benutzerdefinierte Definitionen angeboten werden, sind "Importieren", "Exportieren" und "Löschen".

Löschen von benutzerdefinierten Definitionen

Wenn eine benutzerdefinierte Definition nicht mehr benötigt wird, können Sie sie löschen. Beim Löschen der benutzerdefinierten Definition werden ihr Inhalt und die mit ihr verknüpften Erkennungsregeln aus der Coredatenbank und dem Fenster des Extras "Patch und Compliance" gelöscht. (Die Definitionsinformationen werden beim Exportieren nicht entfernt).

Wie beim Löschen bekannter Anfälligkeitsinformationen der IT-Anbieter werden auch beim Löschen benutzerdefinierter Definitionen keine gedownloadeten, mit der Definition verknüpften Patchdateien entfernt. Patchdateien müssen manuell aus dem Patchrepository entfernt werden.

Um benutzerdefinierte Definitionen zu löschen, wählen Sie eine oder mehrere benutzerdefinierte Definitionen aus und klicken dann auf die Schaltfläche **Ausgewählte benutzerdefinierte Definitionen löschen** in der Symbolleiste.

HINWEIS: Wiederherstellen benutzerdefinierter Definitionen, die exportiert wurden
Wenn Sie eine benutzerdefinierte Definition löschen, die zuvor als XML-Datei exportiert wurde, können Sie diese Definition wiederherstellen, indem Sie sie mithilfe des Extras "Patch und Compliance" wieder importieren.

Importieren und Exportieren von benutzerdefinierten Definitionen

Das Extra "Patch und Compliance" bietet eine Möglichkeit, benutzerdefinierte Definitionen und die mit ihnen verknüpften Erkennungsregeln zu importieren und exportieren. Bekannte Anfälligkeitsdefinitionen von IT-Anbietern können Sie nicht importieren oder exportieren.

Benutzerdefinierte Definitionen werden als XML-Dateien exportiert und importiert.

Das Importieren und Exportieren ist nützlich, wenn Sie benutzerdefinierte Definitionen anderen Coreserver zur Verfügung stellen möchten. Das Exportieren bietet Ihnen die Möglichkeit, eine Sicherungskopie einer Definition zu speichern, die Sie vorübergehend aus der Coredatenbank entfernen möchten.

Sie können die Export-/Importfunktion auch dazu verwenden, eine Definition zu exportieren, die exportierte Datei manuell als Vorlage zu bearbeiten, mehrere Varianten der Definition zu speichern und dann die neuen Definitionen zu importieren. Wenn es sich um eine komplexe Definition handelt, ist dieses Vorgehen möglicherweise schneller und einfacher als das Erstellen mehrerer Definitionen in der Konsole.

So exportieren Sie benutzerdefinierte Definitionen

1. Wählen Sie von einer der Listen mit benutzerdefinierten Definitionen eine oder mehrere benutzerdefinierte Definitionen aus.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Exportieren**. (Alternativ dazu können Sie auch mit der rechten Maustaste auf die ausgewählten Definitionen und dann auf **Exportieren** klicken.)
3. Geben Sie den Pfad zum Ordner ein, aus dem Sie die Definitionen als einzelne XML-Datei exportieren möchten.
4. Wenn Sie die Definitionen zu einem früheren Zeitpunkt in den angegebenen Speicherort exportiert hatten und sie jetzt überschreiben möchten, klicken Sie auf **Vorhandene Definitionen überschreiben**.
5. Klicken Sie auf **Export** und überprüfen Sie im Fenster "Exportstatus", ob die Definitionen erfolgreich exportiert wurden.
   HINWEIS: Eine exportierte Definition bleibt weiterhin in der Coredatenbank bestehen und wird deshalb auch nach wie vor in der Ihrem Status entsprechenden Gruppe "Benutzerdefinierte Definitionen" angezeigt: "Nicht zugewiesen", "Scannen" oder "Nicht scannen".
6. Klicken Sie auf **Schließen**.

So importieren Sie benutzerdefinierte Definitionen

1. Klicken Sie in "Patch und Compliance" auf die Schaltfläche **Benutzerdefinierte Definitionen importieren** der Symbolleiste.
2. Suchen und wählen Sie mindestens eine Definition aus (in der XML-Datei, die Sie importieren möchten) und klicken Sie dann auf **Öffnen**. Wenn die Definition bereits in der Coredatenbank existiert, werden Sie aufgefordert, zu bestätigen, dass Sie sie überschreiben möchten. Überprüfen Sie im Statusfenster, ob die Definition erfolgreich importiert wurde.
3. Klicken Sie auf **Schließen**. Importiere Definitionen (neue und aktualisierte) werden in die Gruppe "Nicht zugewiesene benutzerdefinierte Definitionen" eingefügt.

Sicherheitsscans – Übersicht

Bisher bedeutete Sicherheitsscannen, dass die auf einem Gerät aktuell installierten Versionen der betriebssystem- und programmspezifischen Dateien sowie Registrierungsschlüssel auf die neuesten bekannten Anfälligkeiten überprüft wurden, um Sicherheitsrisiken zu identifizieren und zu beseitigen. LANDesk Security Suite bietet erweiterte Sicherheitsinhalte, die es Ihnen ermöglichen, eine noch größere Anzahl aktueller Sicherheitsrisiken und -lücken aufzuspüren und zu reparieren.

Je nach Security Suite Inhaltsabonnement umfasst das Erkennungsspektrum Folgendes:

- Bekannte Anfälligkeiten (für Windows, Mac, Linux und UNIX)
- Benutzerdefinierte Anfälligkeiten (von einem LANDesk Administrator definiert)
- Spyware
- Antivirus-Scanner-Status (Scanner-Engines von Drittanbietern und das Extra "LANDesk Antivirus")
- Viren (Mithilfe des integrierten LANDesk Antivirus-Tools können Sie die neusten Virendefinitionsdateien herunterladen, Antivirus-Scans erstellen und bereitstellen, Antivirus-Scanner-Einstellungen und die dem Benutzer zur Verfügung gestellten Antivirus-Scan-Optionen konfigurieren, Datei- und E-Mail-Schutz in Echtzeit aktivieren und vieles mehr. Weitere Informationen finden Sie unter "LANDesk Antivirus" auf Seite 751.)
- Sicherheitsbedrohungen (Fehler auf lokalem System oder in der Plattformkonfiguration; einschließlich der Firewallerkennung und -konfiguration)
- Blockierte Anwendungen
- LANDesk Softwareupdates
- Treiberupdates
- Softwareupdates

WICHTIG: LANDesk Security Suite-Inhaltsabonnements
Informationen zu den Security Suite-Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.
LANDesk Startseite

Verwandte Themen

"Wie Patch und Compliance nach verschiedenen Sicherheitsrisiken scannt" auf Seite 620

"Erstellen von Tasks für Sicherheits- und Compliancescans" auf Seite 623

"Konfigurieren von Scanoptionen mit Scan- und Reparatureinstellungen" auf Seite 625

"Konfigurieren von Sicherheitsscan-Inhalten" auf Seite 622

"Anzeigen von erkannten Sicherheitsdaten" auf Seite 628

"Sicherheitsreparatur – Übersicht" auf Seite 631

Wie Patch und Compliance nach verschiedenen Sicherheitsrisiken scannt

Die nachstehende Tabelle verdeutlicht, wie der Sicherheitsscanner "Patch und Compliance" nach dem jeweiligen Inhaltstyp sucht:

Beim Scannen nach...	Erfolgt der Scan von Patch und Compliance durch...
LANDesk Softwareupdates	Verwenden der von LANDesk veröffentlichten Softwareupdatedefinitionen, um nach den neuesten LANDesk Softwareversionen zu suchen.
Windows-Anfälligkeiten	Verwenden der von LANDesk veröffentlichten Anfälligkeitsdefinitionen (auf der Basis offizieller Sicherheitsbulletins von Anbietern der IT-Branche), um nach bekannten Betriebssystem- und/oder Anwendungsanfälligkeiten zu suchen.
Macintosh-Anfälligkeiten	Verwenden der von LANDesk veröffentlichten Anfälligkeitsdefinitionen (auf der Basis offizieller Sicherheitsbulletins), um nach bekannten Anfälligkeiten zu suchen.
Linux/UNIX-Anfälligkeiten	Verwenden der von LANDesk veröffentlichten Anfälligkeitsdefinitionen (auf der Basis offizieller Sicherheitsbulletins), um nach bekannten Anfälligkeiten zu suchen.
Benutzerdefinierte Definitionen	Verwenden der von einem LANDesk-Administrator erstellten benutzerdefinierten Anfälligkeitsdefinitionen, um nach einer benutzerdefinierten Plattform, Anwendung, Datei oder Bedingung für eine Registrierungseinstellung zu suchen.
Sicherheitsbedrohungen	Verwenden der von LANDesk veröffentlichten Anfälligkeitsdefinitionen, um nach bekannten Fehler und Schwachstellen in der lokalen Windows-Systemkonfiguration zu suchen. Sie können Sicherheitsbedrohungsdefinitionen mit editierbaren benutzerdefinierten Variablen ändern, um nach bestimmten Bedingungen zu suchen.
Spyware	Verwenden von Spyware-Erkennungsdefinitionen, die nach Spyware-Programmen auf gescannten Geräten suchen. Patch und Compliance verwendet das softmon.exe-Programm des LANDesk Extras "Softwarelizenzüberwachung" für die Überwachung auf Spyware. Sie können auch Spyware-Überwachung und -Blockierung in Echtzeit über die Agentenkonfiguration eines Geräts aktivieren.
Treiberupdates	Verwenden von Treiberupdatedefinitionen Dritter, die nach Treiberversionen suchen.
Softwareupdates	Verwenden von Softwareupdatedefinitionen Dritter, die nach Softwareversionen suchen.

Beim Scannen nach...	Erfolgt der Scan von Patch und Compliance durch...
Antivirus-Updates	Verwenden von Antivirusscanner-Erkennungsdefinitionen (KEINE tatsächlichen Virendefinitions-/Musterdateien), die Folgendes suchen: – Installationen gebräuchlicher Antivirus-Scanner-Engines (einschließlich LANDesk Antivirus) – Scanstatus in Echtzeit (aktiviert oder deaktiviert) – scannerspezifische Musterdateiversionen (aktuell oder veraltet) – Datum des letzten Scans (liegt der letzte Scan innerhalb der vom Administrator angegebenen maximal zulässigen Zeitspanne)
Blockierte Anwendungen	Verwendet von LANDesk veröffentlichte Anwendungsdefinitionen (oder benutzerdefinierte Programmdefinitionen), um den Endbenutzerzugriff auf die Anwendung sofort zu blockieren, indem die lokale Registrierung bearbeitet wird. Die Reparatur ist *kein* separater Vorgang. Patch und Compliance verwendet das softmon.exe-Programm des Lizenzüberwachungstools von LANDesk Software, um Zugriff auf spezifische Programmdateien zu verweigern (selbst wenn der Name der ausführbaren Datei geändert wurde), indem die Dateiheader-Informationen gelesen werden.

Wenn Sie wissen wollen, wie Patch und Compliance diese unterschiedlichen Inhaltstypen repariert, lesen Sie "Reparaturmethoden" auf Seite 635.

Konfigurieren von Sicherheitsscan-Inhalten

Nachdem Sie die gedownloadeten Definitionen durchgesehen und entschieden haben, wonach gescannt werden soll, können Sie auf verwalteten Geräten angepasste Sicherheitsanalysen durchführen, indem Sie Definitionen in ihre jeweiligen Scangruppen verschieben. Während der Ausführung liest der Sicherheitsscanner standardmäßig die Einträge der Gruppe "Scannen" und sucht nach diesen spezifischen Definitionen (jedoch *nur*, wenn dieser Typ in den Scan- und Reparatureinstellungen des Tasks ausgewählt ist). Vor dem Scannen von Geräten sollten Sie immer sicherstellen, dass sich die entsprechenden Definitionen in der Gruppe "Scannen" befinden. Definitionen lassen sich jederzeit manuell in die Gruppe "Scannen" verschieben oder daraus entfernen.

Überdies können Sie Sicherheitsinhalte aktualisieren; dies führt automatisch dazu, dass neue Definitionen in die Gruppe "Scannen" eingefügt werden.

WICHTIG: Blockierte Anwendungen werden standardmäßig in die Gruppe "Nicht zugewiesen" eingefügt
Denken Sie daran, dass der Anwendungstyp "Blockierte Anwendung" anders gehandhabt wird als die anderen Typen. Definitionen für blockierte Anwendungen werden standardmäßig in die Gruppe "Nicht zugewiesen" eingefügt, und nicht in die Gruppe "Scannen".

Sicherheitsscans fügen Patch- und Compliance-Informationen zum Inventar eines Geräts in der Coredatenbank hinzu. Diese Informationen können zur Erzeugung spezifischer Abfragen, Richtlinien und Berichte verwendet werden. Zeigen Sie diese Informationen an, indem Sie mit der rechten Maustaste auf das betreffende Gerät und dann auf **Sicherheits- und Patchinformationen** klicken.

VORSICHT: Verschieben von Definitionen aus der Gruppe "Scannen"
Wenn Sie Definitionen aus der Gruppe "Scannen" in die Gruppe "Nicht scannen" verschieben, werden die aktuellen Analysedaten für die Definition (Informationen in der Coredatenbank, die darüber Auskunft geben, welche gescannten Geräte diese Definitionen erkannt haben) aus der Coredatenbank entfernt und stehen somit nicht mehr im Dialogfeld "Eigenschaften" einer Definition oder im Dialogfeld "Sicherheits- und Patchinformationen" des Geräts zur Verfügung. Um diese Informationen wiederherzustellen, müssten Sie die Definitionen wieder in die Gruppe "Scannen" verschieben und den Scan erneut ausführen.

Erstellen von Tasks für Sicherheits- und Compliancescans

Der Sicherheitsscan kann direkt auf einem Server ausgeführt werden. (Klicken Sie auf **Start > Programme > LANDesk Management > Sicherheitsscan**). Der Sicherheitsscan kann auch als geplanter Task oder als Richtlinie vom Coreserver aus ausgeführt werden.

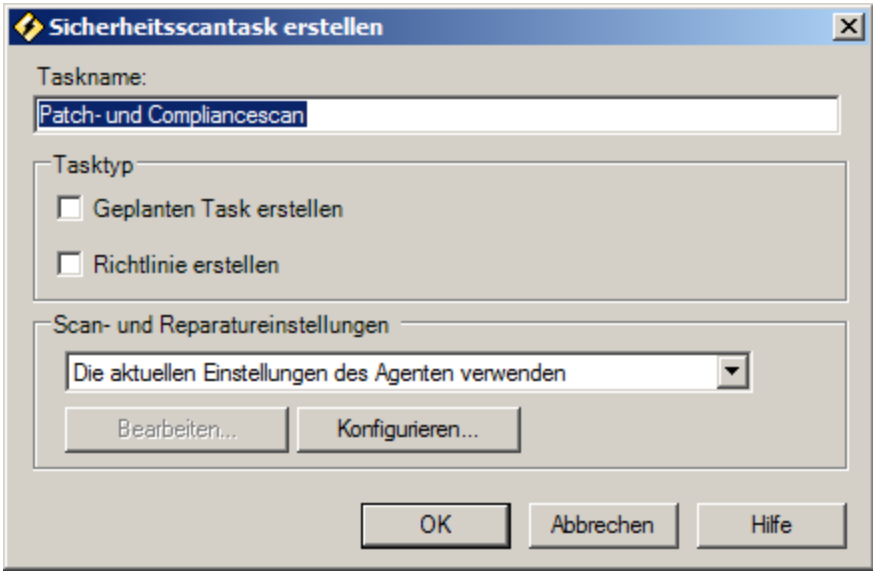
WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Sicherheitskonfigurationen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Geplante Tasks sind einer Pushverteilung nicht unähnlich, da der Task vom Coreserver per Pushprozedur an Geräte übermittelt wird. Eine Richtlinie ähnelt dagegen eher einer Pullverteilung, da der Richtlinienagent auf dem Gerät den Coreserver auf relevante Richtlinien durchsucht und das Patch dann mittels Pullprozedur vom Coreserver abruft.

So erstellen Sie einen Sicherheitsscan-Task

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Stellen Sie sicher, dass der Sicherheitsinhalt kürzlich aktualisiert wurde.
3. Stellen Sie sicher, dass die Gruppe **Scannen** nur diejenigen Definitionen beinhaltet, nach denen Sie scannen möchten.

4. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitsscan**. Das Dialogfeld "Sicherheitsscantask erstellen" wird geöffnet.



5. Geben Sie einen Namen für den Scan ein.
6. Geben Sie an, ob der Scan ein geplanter Task, ein richtlinienbasierter Scan oder beides ist.
7. Wählen Sie eine der Scan- und Reparatureinstellungen aus der Liste der verfügbaren Einstellungen aus (oder erstellen Sie benutzerdefinierte Einstellungen für diesen Scan), um festzulegen, wie der Scan auf Endbenutzergeräten ausgeführt wird.
8. Klicken Sie auf **OK**. Für einen Scan, der als geplanter Task ausgeführt wird, können Sie jetzt Zielgeräte hinzufügen und die Zeitplanoptionen im Extra "Geplante Tasks" konfigurieren.

HINWEIS: Compliance-Sicherheitsscans
Das Extra "Patch und Compliance" bietet Ihnen die Möglichkeit, einen auf Compliance ausgerichteten Scantask zu erstellen und zu konfigurieren, der Zielgeräte auf Konformität mit benutzerdefinierten Sicherheitsrichtlinien scannt. Ein Compliancescan basiert auf dem Inhalt der Gruppe **Compliance** (und den in den Compliance-Einstellungen spezifizierten Optionen) und kann als geplanter Task oder als Richtlinie ausgeführt und sogar von LANDesk Antivirus initiiert werden, wenn ein Virus erkannt wird, der nicht entfernt oder unter Quarantäne gestellt werden kann.

Ausführen eines On-Demand-Sicherheits- oder Compliancescans

Sie können auch einen sofortigen "On-Demand"-Scan auf einem oder mehreren Zielgeräten veranlassen.

Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät (oder auf bis zu 20 Geräte gleichzeitig), klicken Sie auf **Sicherheits-/Compliancescan jetzt ausführen...**, wählen Sie eine Scan- und Reparatureinstellung sowie den Scantyp aus und klicken dann auf **OK**.

Informationen über die Sicherheitsscan-Protokolldatei

Der Sicherheitsscanner legt eine Protokolldatei namens **vulscan.log** mit Daten über den aktuellsten Scan auf dem Gerät an und speichert zudem die letzten fünf Protokolldateien in chronologischer Reihenfolge und nach Nummern sortiert. Diese Protokolldateien zeichnen nützliche Informationen zur Uhrzeit des Scans, Sprache, Plattform und den vom Scan ausgeführten Prozessen auf.

Anzeigen der letzten Sicherheitsscandaten im Geräteinventar

Um nachzuprüfen, wann der letzte Sicherheitsscan auf einem Gerät ausgeführt wurde, klicken Sie mit der rechten Maustaste auf das Gerät, klicken auf **Inventar** und blättern dann mit der Bildlaufleiste nach unten zum Eintrag **Datum des letzten Scans** im rechten Fensterausschnitt der Inventaransicht.

Konfigurieren von Scanoptionen mit Scan- und Reparatureinstellungen

Mit Patch und Compliance bestimmen Sie bis ins letzte Detail, was die Endbenutzer sehen, wie und wann ein Neustart erfolgt und welche Stufe der Interaktion dem Endbenutzer erteilt wird, während der Sicherheitsscanner auf Geräten läuft. Beispiel: Je nach Zweck oder geplantem Ausführungszeitpunkt eines Scans empfiehlt es sich möglicherweise, den Endanwender über den Scanverlauf zu informieren und ihm die Möglichkeit zu geben, einen Analysescan oder eine Patchbereitstellungsreparatur abzubrechen oder auf einen späteren Zeitpunkt zu verlegen. Sie können dies tun, indem Sie Scan- und Reparatureinstellungen erstellen und anwenden.

In den Scan- und Reparatureinstellungen entscheiden Sie zudem über den Inhalt eines Sicherheitsscans, indem Sie bestimmte Definitionstypen auswählen.

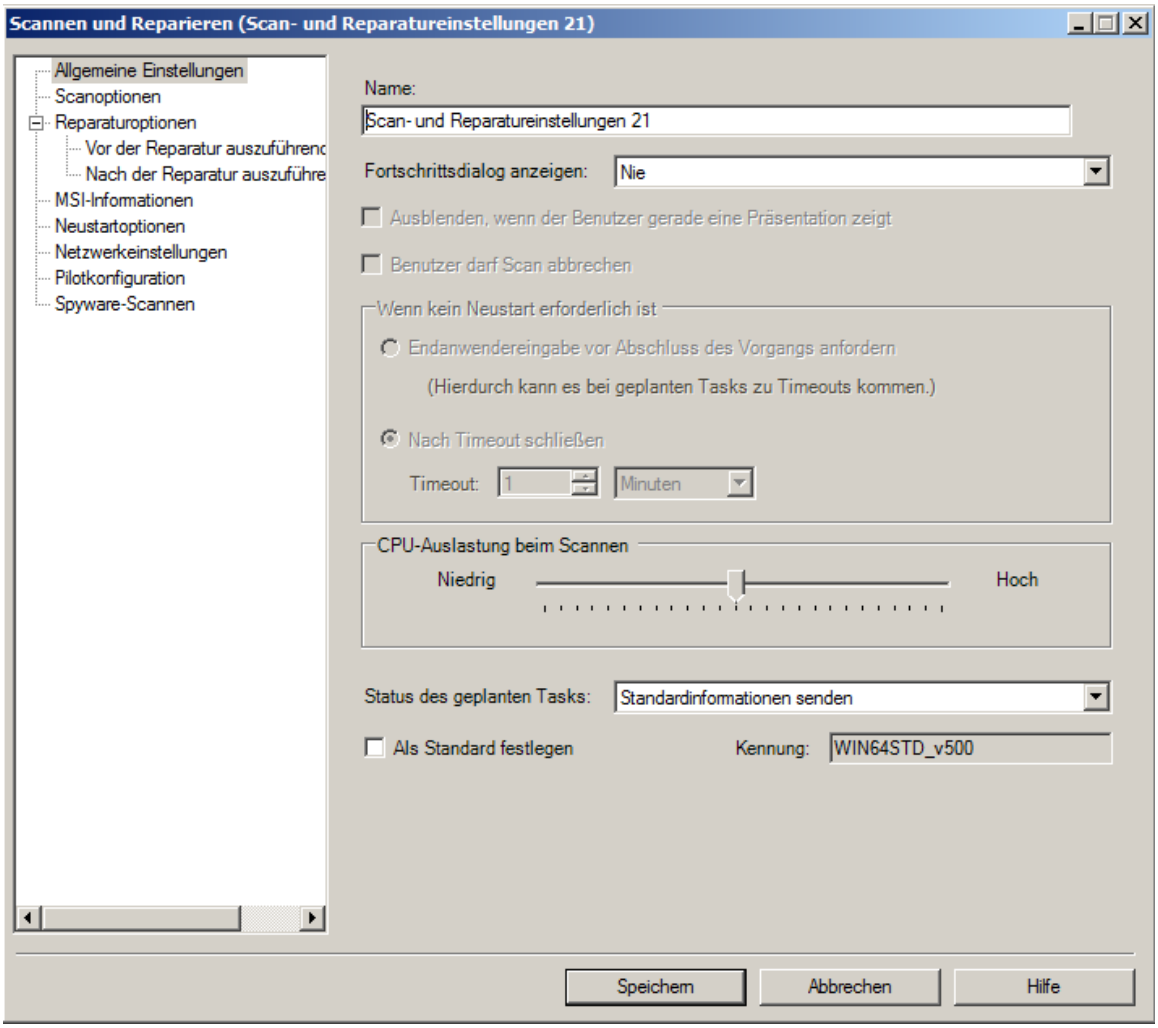
Sie können Scan- und Reparatureinstellungen (einen gespeicherten Satz konfigurierter Optionen) erstellen und auf Scantasks anwenden. Sie können beliebig viele Scan- und Reparatureinstellungen erstellen. Einige Scan- und Reparatureinstellungen eignen sich möglicherweise für eine Reihe unterschiedlicher Scan- oder Reparaturtasks, während andere u. U. nur bei einem bestimmten Task zum Einsatz kommen.

Alle von Ihnen erstellten Scan- und Reparatureinstellungen werden in der Gruppe **Scannen und Reparieren** unter **Einstellungen** in der Strukturansicht gespeichert.

So erstellen Sie Scan- und Reparatureinstellungen

1. Klicken Sie im Fenster des Extras **Patch und Compliance** auf die Symbolleistenschaltfläche **Einstellungen konfigurieren** und klicken Sie dann auf **Scan- und Reparatureinstellungen**.

2. Klicken Sie auf **Neu**. Alternativ können Sie auch in jedem beliebigen Task-Dialogfeld, das es Ihnen ermöglicht, Scan- und Reparatureinstellungen zu aktivieren, auf **Bearbeiten** oder **Konfigurieren** klicken.



3. Geben Sie einen Namen für die Scan- und Reparatureinstellungen ein.
4. Geben Sie die Einstellungen wie gewünscht auf den Seiten für den speziellen Task (Scan, Reparatur, Neustart) ein. Für weitere Informationen zu einer Option klicken Sie auf **Hilfe**.

Nachdem Sie Scan- und Reparatureinstellungen konfiguriert haben, können Sie sie Sicherheitsscan-Tasks, Reparaturtasks, Deinstallationstasks, Neustart-Tasks und Einstellungsänderungstasks zuweisen.

HINWEIS: Compliance-Einstellungen
Mit dem Extra "Patch und Compliance" können Sie auch spezifische Einstellungen für Compliance erstellen, die festlegen, wann der häufig ausgeführte Sicherheitsscan ausgeführt wird und wie mit erkannten Risiken verfahren wird. Ein Compliancescan basiert auf dem Inhalt der Gruppe **Compliance** (und den in den Compliance-Einstellungen spezifizierten Optionen) und kann als geplanter Task oder als Richtlinie ausgeführt und sogar von LANDesk Antivirus initiiert werden, wenn ein Virus erkannt wird, der

nicht entfernt oder unter Quarantäne gestellt werden kann.

Ändern der Scan- und Reparatur-Standardeinstellungen eines Geräts

Die Scan- und Reparatur-Standardeinstellungen eines Geräts werden als Teil der ursprünglichen Agentenkonfiguration bereitgestellt. Wenn ein Task mit einer anderen Scan- und Reparatureinstellung verknüpft ist oder ihm eine solche Einstellung zugewiesen wurde, werden die Standardeinstellungen überschrieben. Sie können die Standardeinstellungen des Geräts verwenden, indem Sie sie beim Erstellen eines Tasks auswählen.

Irgendwann einmal möchten Sie vielleicht diese Scan- und Reparatur-Standardeinstellungen auf bestimmten Geräten ändern. Patch und Compliance bietet eine Möglichkeit, diese Änderung vorzunehmen, ohne erneut eine komplett neue und vollständige Agentenkonfiguration bereitstellen zu müssen. Verwenden Sie hierfür den Task **Einstellungen ändern** aus der Liste der Symbolleistenschaltfläche **Task erstellen**.

In das eingeblendete Dialogfeld können Sie einen eindeutigen Namen für den Task eingeben, festlegen, ob es sich um einen geplanten Task oder eine Richtlinie handelt, und entweder eine vorhandene Scan- und Reparatureinstellung als Standard auswählen oder mithilfe der Schaltfläche **Bearbeiten** eine neue Scan- und Reparatureinstellung als Standard für Zielgeräte erstellen.

Verwenden von benutzerdefinierten Variablen und Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen

Mit benutzerdefinierten Variablen können Sie das Scannen auf Sicherheitsbedrohungen optimieren, indem Sie die Werte einer oder mehrerer Einstellungen so ändern, dass der Scanner nach von Ihnen definierten Bedingungen sucht und das Gerät nur dann als anfällig erkennt, wenn diese spezielle Bedingung erfüllt ist (d. h. der von Ihnen angegebene Wert vorgefunden wird). Einige Definitionen für Sicherheitsbedrohungen der Systemkonfiguration verfügen beispielsweise über Einstellungen, die Sie ändern können, bevor Sie sie in einem Sicherheitsscan einschließen. Normalerweise verfügen Virenschutzdefinitionen auch über Einstellungen für benutzerdefinierte Variablen.

WICHTIG: Das Recht "Benutzerdefinierte Variablen bearbeiten" ist erforderlich
Um Einstellungen benutzerdefinierter Variablen bearbeiten zu können, muss der LANDesk Benutzer über das rollenbasierte Administrationsrecht "Benutzerdefinierte Variablen bearbeiten" verfügen. Rechte werden mit dem Extra **Benutzer** konfiguriert.

Jede Sicherheitsdefinition, die über benutzerdefinierte Variablen verfügt, besitzt einen eindeutigen Satz spezifischer änderbarer Werte. In jedem Fall werden auf der Seite **Benutzerdefinierte Variablen** jedoch die folgenden Informationen zu sehen sein:

- **Name:** Identifiziert die benutzerdefinierte Variable. Der Name kann nicht geändert werden.
- **Wert:** Gibt den aktuellen Wert der benutzerdefinierten Variable an. Sie können auf dieses Feld doppelklicken, um den Wert zu ändern, es sei denn, die Variable ist schreibgeschützt.
- **Beschreibung:** Stellt zusätzliche nützliche Informationen zur benutzerdefinierten Variable bereit, die vom Autor der Definition stammen.
- **Standardwert:** Stellt den Standardwert bereit, falls Sie Einstellungen geändert haben und den ursprünglichen Wert wiederherstellen möchten.

Um eine benutzerdefinierte Variable zu ändern, doppelklicken Sie auf das Feld **Wert** und wählen entweder einen Wert aus, wenn es eine Liste gibt, oder bearbeiten den Wert ansonsten manuell und klicken dann auf **Übernehmen**. Beachten Sie, dass einige Variablen schreibgeschützt sind und nicht bearbeitet werden können (dies wird normalerweise in der Beschreibung vermerkt).

HINWEIS: Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen
In manchen Situationen sollten Sie benutzerdefinierte Variableneinstellungen ggf. ignorieren oder – anders ausgedrückt – eine Ausnahme von der Regel erstellen. Hierfür steht in eine Funktion mit dem Namen "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen" zur Verfügung. Mithilfe der Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen können Sie entscheiden, welche benutzerdefinierten Variablen beim Scannen von Geräten ignoriert werden, damit sie nicht als anfällig erkannt und repariert werden, selbst wenn sie eigentlich die Bedingungen der Erkennungsregeln einer Definition erfüllen. Ein Benutzer muss berechtigt sein, benutzerdefinierte Variablen zu bearbeiten, damit er Einstellungen zur Außerkraftsetzung für benutzerdefinierte Variablen erstellen oder bearbeiten kann. Sie können beliebig viele Einstellungen zur Außerkraftsetzung benutzerdefinierter Variablen erstellen und diese dann mit einem Task vom Typ **Einstellungen ändern** auf Geräte anwenden. Weitere Informationen hierzu finden Sie unter "Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen"" auf Seite 685.

Anzeigen von erkannten Sicherheitsdaten

Wenn der Sicherheitsscanner eine der ausgewählten Definitionen auf einem Zielgerät erkennt, wird diese Information an den Coreserver weitergegeben. Sie können sich einer der folgenden Methoden bedienen, um nach Abschluss eines Scans erkannte Sicherheitsdaten anzuzeigen:

Nach der Gruppe "Erkannt"

Wählen Sie im Fenster des Extras "Patch und Compliance" die Gruppe **Erkannt** aus, um eine vollständige Liste aller Definitionen einzublenden, die während des letzten Scans erkannt wurden.

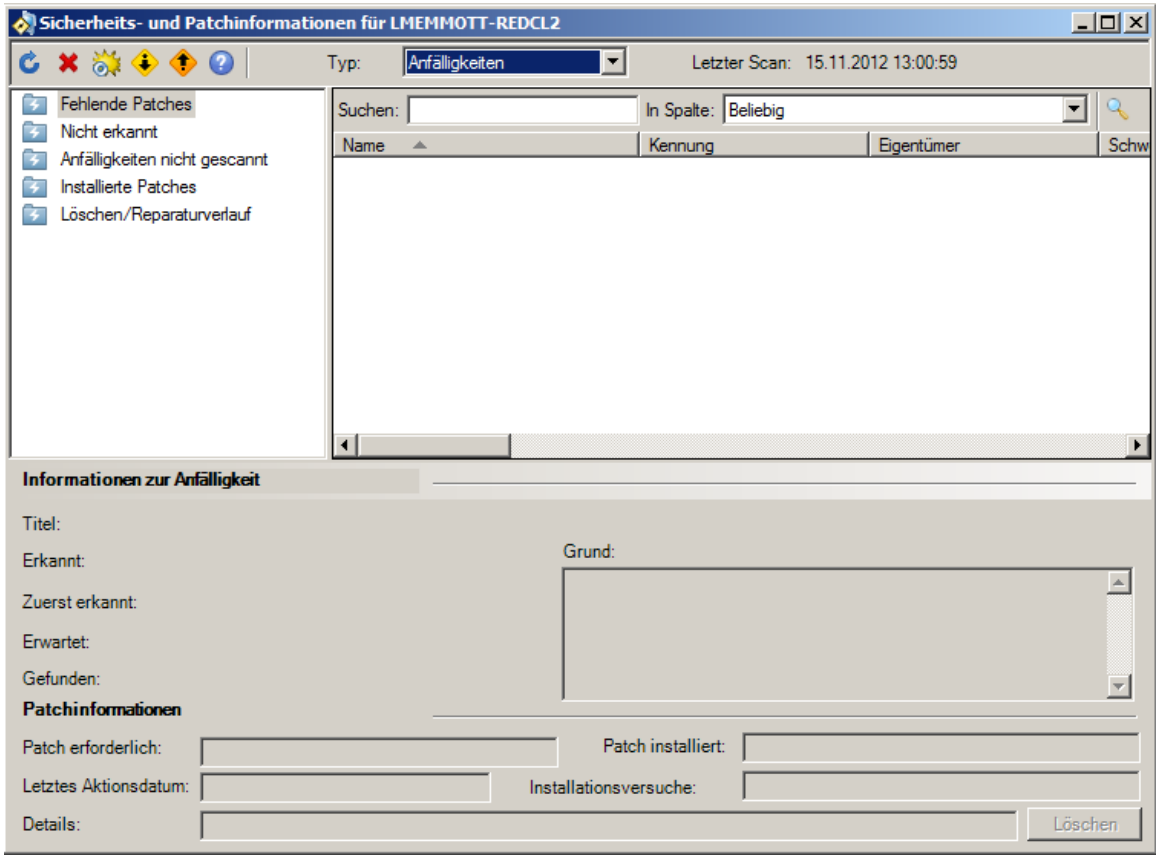
In der Spalte "Gescannt" wird angezeigt, wie viele Geräte auf eine Definition überprüft wurden; aus der Spalte "Erkannt" geht hervor, wie viele dieser Geräte von dieser Definition betroffen sind.

Nach einer Definition

Klicken Sie mit der rechten Maustaste auf eine Definition und klicken Sie dann auf **Betroffene Computer**, um eine Liste der Geräte anzuzeigen, auf denen die Definition während des jüngsten Scans erkannt wurde.

Nach dem Dialogfeld "Sicherheits- und Patchinformationen" des Geräts

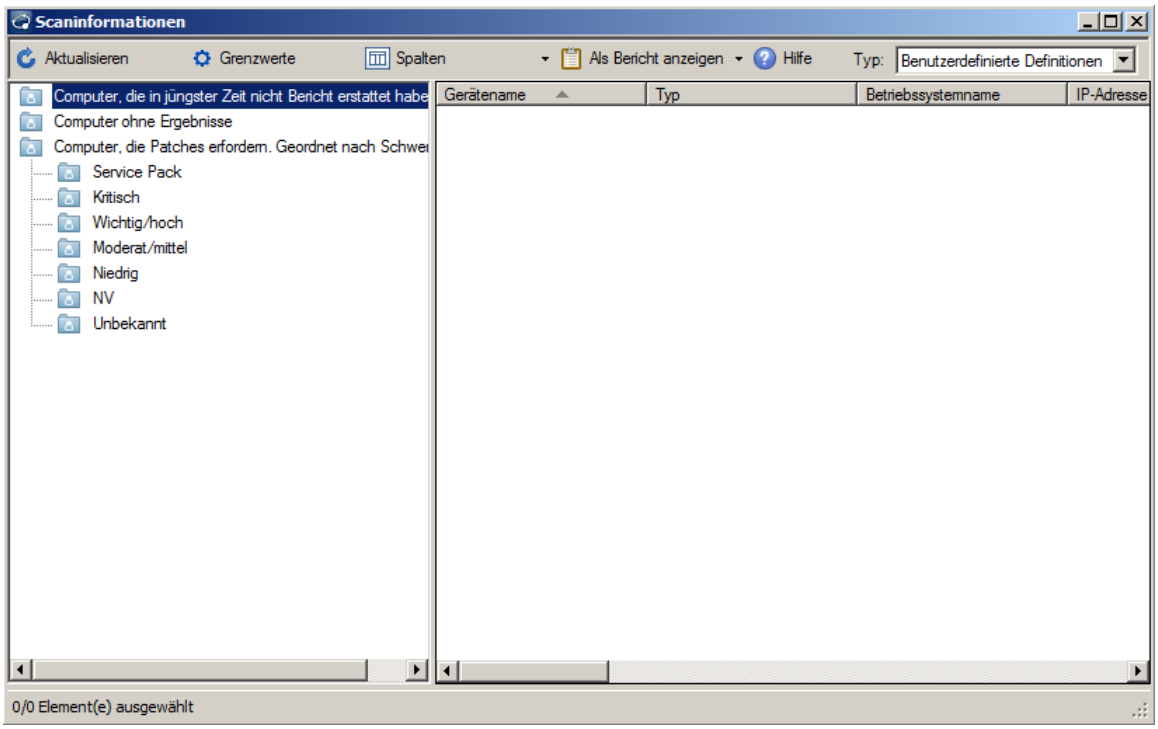
Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf ein bestimmtes Gerät und klicken Sie dann auf **Sicherheits- und Patchinformationen**, um detaillierte Angaben zur Sicherheitsanalyse und zum Status der Patchbereitstellung für dieses Gerät anzuzeigen.



Sie können auch mehrere Geräte in der Netzwerkansicht auswählen, mit der rechten Maustaste auf die Gruppe klicken und dann auf **Sicherheits- und Patchinformationen** klicken, um eine Liste der Definitionen anzuzeigen, die auf einem oder mehreren dieser Geräte erkannt wurden. Wenn Sie eine Definition in dieser Liste auswählen, werden im unteren Fensterausschnitt diejenigen Geräte angezeigt, auf denen die betreffende Definition während des jüngsten Scans erkannt wurde.

Nach dem Dialogfeld "Scaninformationen"

Klicken Sie im Fenster des Extras "Patch und Compliance" auf die Symbolleistenschaltfläche **Scaninformationen**, um Details zu Aktivitäten und zum Status der Patchbereitstellung für gescannte Geräte in Ihrem Netzwerk anzuzeigen. Sie können Scanergebnisse für Computer anzeigen, die in jüngster Zeit nicht Bericht erstattet haben, zu Computern ohne Ergebnisse und zu Computern, die Patches erfordern, geordnet nach Schweregrad.



Weiterleiten von Sicherheitsscanergebnissen an einen Rollup-Core

Wenn Sie in einem großen verteilen Unternehmensnetzwerk arbeiten, sollten Sie die neuesten Sicherheitsscanergebnisse an einen Rollup-Core-Server, der seinen Standort in einer bestimmten Region hat, weiterleiten, um auf diese Weise den Echtzeitzugriff auf Anfälligkeitsinformationen für Ihre sämtlichen verwalteten Geräte zu verbessern. Sie können die automatische und sofortige Weiterleitung der Ergebnisse von Sicherheitsscans aktivieren, indem Sie die erforderlichen Rollup-Core-Einstellungen im Extra "Patch und Compliance" definieren.

Bei jedem Ausführen des Sicherheitsscanners wird eine Scanergebnisdatei in einen Ordner namens "VulscanResults" auf dem Coreserver geschrieben. Ferner wird der LANDesk Security Suite-Webdienst benachrichtigt, der die Datei dann zur Coredatenbank hinzufügt. Wenn die Rollup-Core-Einstellungen aktiviert sind und ein gültiger Rollup-Core erkannt wird, liest der Rollup-Core die Scanergebnisdatei in seine eigene Datenbank, sodass der Zugriff auf kritische Anfälligkeitsdaten beschleunigt wird.

So aktivieren Sie die sofortige Weiterleitung von Sicherheitsscanergebnissen an einen Rollup-Core

1. Klicken Sie im Fenster des Extras **Patch und Compliance** auf die Symbolleistenschaltfläche **Einstellungen konfigurieren** und klicken Sie dann auf **Rollup Core-Einstellungen**.
2. Aktivieren Sie das Kontrollkästchen **Scanergebnisse sofort an Rollup-Core senden**.
3. Geben Sie den Namen des Rollup-Cores ein, an den die neuesten Sicherheitsscanergebnisse weitergeleitet werden sollen.
4. Wenn die Scanergebnisdatei in die Standard-URL (Speicherort auf dem Rollup-Core) geschrieben werden soll, aktivieren Sie das Kontrollkästchen **Standard-Rollup-URL verwenden**. Andernfalls deaktivieren Sie das Kontrollkästchen und geben Sie die gewünschte Adresse ein.

Sicherheitsreparatur – Übersicht

Dieser Abschnitt gibt einen Überblick über das Reparieren von Geräten, bei denen Sicherheitsrisiken erkannt wurden.

Nachdem Sie den Sicherheitsinhalt für die von Ihnen lizenzierten oder abonnierten Inhaltstypen aktualisiert haben, Geräte gescannt und entschieden haben, welche erkannten Schwachstellen repariert werden müssen, sowie Patches heruntergeladen haben, besteht der nächste Schritt bei der Implementierung der Patch und Compliance-Sicherheit darin, das Sicherheitsproblem zu beseitigen (oder zu reparieren).

Reparaturlösungen und -aktionen unterscheiden sich, je nachdem, welche Art von Sicherheitsrisiko vorliegt. Einige Reparaturen lassen sich darüber hinaus remote mit dem Extra "Patch und Compliance" ausführen, während andere Reparaturtasks manuell ausgeführt werden müssen. Anfälligkeiten werden beispielsweise repariert, indem Sie die erforderlichen Sicherheitspatches auf betroffenen Geräten bereitstellen und installieren, während Spyware repariert wird, indem Sie die Spyware entfernen. Eine Sicherheitsbedrohung der Systemkonfiguration wird normalerweise durch die Bearbeitung der Registrierungsdatenbank oder das Ändern anderer plattformspezifischer Einstellungen repariert.

Reparaturen für verschiedene Sicherheitsrisiken

Nachstehend wird der Reparaturvorgang für alle Sicherheitsrisiken (bzw. Inhaltstypen) beschrieben.

Bekannte Anfälligkeiten

Für bekannte Anfälligkeiten besteht die Reparatur darin, das zutreffende Sicherheitspatch zu verteilen und zu installieren. Die Reparatur von Windows- und Macintosh-Anfälligkeiten kann über die Konsole durchgeführt werden - als geplanter Task, als richtlinienbasierte Reparatur oder als Autofix-Scan. Die Reparatur von Linux- und UNIX-Anfälligkeiten dagegen muss manuell am betroffenen Gerät vorgenommen werden.

Benutzerdefinierte Definitionen

Bei benutzerdefinierten Definitionen kann die Reparatur aus dem Verteilen eines benutzerdefinierten Patches oder Skripts bestehen, mit dem die Schwachstelle adressiert wird. Benutzerdefinierte Reparaturtasks für Anfälligkeiten können wie Reparaturen von bekannten Anfälligkeiten von der Konsole aus durchgeführt werden.

LANDesk Softwareupdates

Für LANDesk Softwareupdates bedeutet Reparieren, dass das richtige Versionsupgrade installiert wird. Dieser Vorgang lässt sich über die Konsole abwickeln.

Sicherheitsbedrohungen

Bei Sicherheitsbedrohungen (Konfigurationsfehlern und Schwachstellen auf lokalen Windows-Systemen und -Plattformen) bedeutet "Reparatur" die Anwendung von Konfigurationseinstellungen, die durch Windows-Firewalleinstellungen oder vordefinierte Sicherheitsbedrohungsdefinitionen spezifiziert sind. Dieser Vorgang lässt sich über die Konsole abwickeln. Sie können aber auch Sicherheitsbedrohungsdefinitionen mit editierbaren benutzerdefinierten Variablen verwenden, um speziell angepasste Einstellungen anzuwenden.

Manche Sicherheitsbedrohungen müssen manuell am betroffenen Gerät repariert werden. Wenn Sie wissen möchten, ob eine Sicherheitsbedrohung von der Konsole aus repariert werden kann, schauen Sie in der Listenansicht des Elements nach, auf welchen Wert die Spalte "Reparierbar" gesetzt ist ("Ja" oder "Nein").

Firewallerkennung und -konfiguration (unter Verwendung von Windows-Firewalleinstellungen und Sicherheitsbedrohungsdefinitionen)

Bei Windows-Firewallkonfigurationen bedeutet "Reparatur" die Anwendung von Konfigurationseinstellungen, die durch Windows-Firewalleinstellungen oder vordefinierte Sicherheitsbedrohungsdefinitionen spezifiziert sind.

Windows-Firewalleinstellungen sind mit einem Einstellungsänderungs-Task verknüpft, mit dem Sie die Firewall aktivieren/deaktivieren und Firewalleinstellungen konfigurieren können, einschließlich Ausnahmen, Eingangsregeln und Ausgangsregeln (für Dienste, Anschlüsse und Programme) auf Zielgeräten der folgenden Windows-Plattformen:

- Windows 2003/XP
- Windows Vista

LANDesk Security Suite bietet zusätzlich vordefinierte Sicherheitsbedrohungsdefinitionen, mit denen Sie die Firewalleinstellungen auf verwalteten Geräten unter bestimmten Windows-Plattformen scannen, erkennen und konfigurieren können. Mit den folgenden Sicherheitsbedrohungsdefinitionen können Sie Firewalleinstellungen scannen und ändern:

- **ST000102:** Sicherheitsbedrohungsdefinition für die Windows-Firewall unter Windows 2003 SP1; Windows XP SP2.
- **ST000015:** Sicherheitsbedrohungsdefinition für die Internetverbindungsfirewall unter Windows 2003 SP1; Windows XP SP2.

Zu den Eigenschaften der Sicherheitsbedrohung der Windows-Firewall gehören benutzerdefinierte Variablen, mit deren Hilfe Sie Windows-Firewalleinstellungen konfigurieren können. Sie können diese Sicherheitsbedrohungsdefinitionen zum Scannen auf Ihre angegebenen Einstellungen verwenden und eine Anfälligkeitsbedingung zurückgeben, falls diese Einstellungen nicht übereinstimmen. Die benutzerdefinierte Definition können Sie dann in einem Reparaturtask dazu verwenden, die Firewall ein- oder auszuschalten oder die Firewalleinstellungen auf dem gescannten Gerät neu zu konfigurieren.

VORSICHT: Windows GPO kann ggf. Firewalleinstellungen ändern
Sie sollten sich der Möglichkeit bewusst sein, dass ein Windows-Gruppenrichtlinienobjekt (GPO) die mit dem Sicherheitsscanner konfigurierten Firewalleinstellungen beeinträchtigt. Die Firewalleinstellungen, die Sie im Dialogfeld "Configure the Windows Firewall security threat's custom variables" (Benutzerdefinierte Variablen der Windows-Firewallsicherheitsbedrohung konfigurieren) definieren und die dann durch eine Sicherheitsscanner-Reparatur implementiert werden, könnten beispielsweise auf ihren ursprünglichen Wert zurückgeführt werden, je nach Definition der Einstellungen in einem aktiven Gruppenrichtlinienobjekt (GPO).

Spyware

Bei Spyware besteht die Reparatur darin, die destruktive Spyware-Anwendung zu entfernen. Dieser Vorgang kann remote von der Konsole aus mit einem Reparaturtask ausgeführt werden.

Sie können Geräte auch die Spyware-Überwachung in Echtzeit (Scannen, Erkennen, Entfernen) konfigurieren. Um die Echtzeit-Spyware-Überwachung einsetzen zu können, müssen Sie die Einstellungen in der Agentenkonfiguration des Geräts aktivieren. Aktivieren Sie auf der Seite **Spyware** des Dialogfeldes **Agentenkonfiguration** die erforderlichen Spyware-Überwachungsoptionen, um die Spyware-Überwachung in Echtzeit und Endanwenderbenachrichtigung zu aktivieren. Die Spyware-Überwachung in Echtzeit verwendet das softmon.exe-Programm des LANDesk Software-Extras "Softwarelizenzüberwachung" für die Überwachung auf Spyware und zum Erstellen von Protokolldateien, die vom Sicherheitsscanner gelesen werden, wenn dieser nach Spyware-Definitionen auf Zielgeräten scannt.

WICHTIG: Die Funktion automatisches Korrigieren muss aktiviert sein, damit die Spyware-Überwachung in Echtzeit ausgeführt werden kann
Damit das Spyware-Scanning in Echtzeit und die Spyware-Erkennung funktioniert, muss für heruntergeladene Spyware-Definitionen die Option zum automatischen Korrigieren aktiviert sein. Sie können die Option zum automatischen Korrigieren für Spyware-Definitionen in der Elementliste im Fenster des Extras "Patch und Compliance" manuell aktivieren. Oder Sie können Spyware-Definitionsupdates konfigurieren, sodass die Option "Automatisches Korrigieren" standardmäßig eingeschaltet ist, wenn Spyware-Definitionen heruntergeladen werden.

Blockierte Anwendungen

Bei blockierten Anwendungen ist die Reparatur *kein* separater Task. Das Verweigern einer Anwendung findet als Teil des eigentlichen Sicherheitsscans statt, indem die Registrierung auf dem lokalen Festplattenlaufwerk so bearbeitet wird, dass der Benutzerzugriff auf diese nicht autorisierten Anwendungen deaktiviert wird.

Patch und Compliance verwendet das softmon.exe-Programm um Zugriff auf spezifische Programmdateien zu verweigern (selbst wenn der Name der ausführbaren Datei geändert wurde), indem die Dateiheader-Informationen gelesen werden.

Antivirus-Updates

Antivirus-Updates stehen für mehrere gebräuchliche Antivirus-Produkte, einschließlich LANDesk Antivirus, zur Verfügung. Sehen Sie die Liste mit den **Definitionstypen** im Dialogfeld **Updates downloaden** durch, um zu erfahren, welche Antivirus-Scanner-Engines unterstützt werden, d. h., für welche Antivirus-Scanner-Engines Sie Erkennungsdefinitionen herunterladen können.

HINWEIS: Vom Antivirus-Scanner erkannter Inhalt im Vergleich zu Virendefinitionsinhalt
Antivirus-Updates erstrecken sich nicht auf die eigentlichen Virendefinitionsdateien (oder Musterdateien). Wenn Sie Antivirus-Updates eines anderen Herstellers herunterladen, wird nur von Scannern erkannter Inhalt in das Standardrepository heruntergeladen, scannerspezifische Virendefinitionsdateien werden dagegen NICHT heruntergeladen. Wenn Sie jedoch LANDesk Antivirus-Updates herunterladen, werden *sowohl* vom Scanner erkannte Inhalte *als auch* die LANDesk Antivirus-spezifischen Virendefinitionsdateien heruntergeladen. LANDesk Antivirus-Virendefinitionsdateien werden in einen separaten Speicherort auf dem Coreserver heruntergeladen. Das Standardrepository für Virendefinitionsdateien ist der Ordner \LDLogon\Antivirus\Bases.

Antivirus-Updates sind Scannerdefinitionen, die Folgendes erkennen:

- Installation von gängigen Antivirus-Scanner-Engines (einschließlich des Extras "LANDesk Antivirus")
- Scanstatus in Echtzeit (aktiviert oder deaktiviert)
- Scannerspezifische Musterdateiversionen (auf dem neuesten Stand oder veraltet)

- Datum des letzten Scans (ob der letzte Scan innerhalb des vom Administrator festgelegten maximal zulässigen Zeitraums erfolgte)

Beim Bereitstellen eines Sicherheitsscans mit Antivirus-Scanner-Erkennungsdefinitionen überprüft der Sicherheitsscanner, ob eine Antivirus-Scanner-Engine auf den verwalteten Geräten installiert ist, ob Echtzeitscans aktiviert oder deaktiviert sind, ob die Musterdateien des Scanners auf dem neuesten Stand sind und wann zuletzt ein Scan auf dem Gerät ausgeführt wurde. Sie können Echtzeitscans remote aktivieren, falls sie ausgeschaltet sind.

Wie Patch und Compliance verschiedene Sicherheitsrisiken repariert

Die nachstehende Tabelle verdeutlicht, wie Patch und Compliance den jeweiligen Sicherheitsrisikotyp repariert:

Inhalt der Reparatur	Art der Patch und Compliance-Reparatur
LANDesk Softwareupdates	Bereitstellen und Installieren des zutreffenden LANDesk Softwareupdates.
Windows-Anfälligkeiten	Bereitstellen und Installieren der erforderlichen Patchdateien (Patchdateien müssen bereits in das lokale Patchrepository gedownloadet worden sein).
Macintosh-Anfälligkeiten	Bereitstellen und Installieren der erforderlichen Patchdateien
Linux/UNIX-Anfälligkeiten	Die Reparatur erfolgt manuell auf dem betroffenen Gerät.
Benutzerdefinierte Definitionen	Bereitstellen und Installieren von Patchdateien, wenn die mit der Definition verknüpfte Erkennungsregel eine Reparatur zulässt und die angegebenen Patchdateien zur Verfügung stehen.
Sicherheitsbedrohungen	Anwenden der Konfigurationseinstellungen, die in der Definition der Sicherheitsbedrohung festgelegt sind. Dieser Vorgang lässt sich über die Konsole abwickeln. Sie können aber auch Sicherheitsbedrohungsdefinitionen mit editierbaren benutzerdefinierten Variablen verwenden, um speziell angepasste Einstellungen anzuwenden. Manche Sicherheitsbedrohungen müssen manuell am betroffenen Gerät repariert werden. Wenn Sie wissen möchten, ob eine Sicherheitsbedrohung von der Konsole aus repariert werden kann, schauen Sie in der Listenansicht des Elements nach, auf welchen Wert die Spalte "Reparierbar" gesetzt ist ("Ja" oder "Nein").
Spyware	Entfernen der erkannten Spyware-Instanz. Weitere Informationen zur Echtzeit-Spyware-Erkennung und -Entfernung finden Sie im Abschnitt "Spyware" weiter oben.
Treiberupdates	Bereitstellen und Installieren des zutreffenden Treiberupdates eines Drittanbieters.

Inhalt der Reparatur	Art der Patch und Compliance-Reparatur
Softwareupdates	Bereitstellen und Installieren des zutreffenden Softwareupdates eines Drittanbieters.
Antivirus-Updates	Gibt Ihnen die Möglichkeit, Echtzeitscans erneut zu aktivieren, falls sie ausgeschaltet waren. Die anderen Antivirus-Scanner-Erkennungsdefinitionen geben Statusinformationen zu spezifischen Antivirus-Scanner-Engine-Installationen, Musterdateiversionen und zum letzten Scandatum zurück (damit in Verbindung stehende Probleme können nicht remote von der Konsole aus korrigiert werden).
Blockierte Anwendungen (veröffentlicht und benutzerdefiniert)	Den Zugriff auf Anwendungen verweigern, selbst wenn sich der Name der Programmdatei geändert hat, indem die Datei-Header-Informationen gelesen werden. Die Reparatur ist in diesem Fall *kein* separater Vorgang. Die Anwendungsverweigerung erfolgt während des Sicherheitsscans. Der Sicherheitsscan verweigert durch Bearbeiten der Registrierung dem Endanwender sofort den Zugriff auf die Anwendung. (Siehe "Rechtshinweis zum Typ "Blockierte Anwendung"" auf Seite 611.)

Wenn Sie wissen wollen, wie Patch und Compliance nach diesen unterschiedlichen Inhaltstypen scannt, lesen Sie "Sicherheitsscans – Übersicht" auf Seite 620.

Reparaturmethoden

Patch und Compliance stellt mehrere Methoden für die Reparatur betroffener Geräte zu Verfügung.

Intelligente Reparatur durch gezielte Patchbereitstellung

Patch und Compliance führt eine intelligente Reparatur durch, indem nur diejenigen Patches installiert werden, die auf dem jeweiligen Gerät benötigt werden. Es werden also nicht sämtliche Patches installiert, auf die sämtliche im Reparaturauftrag enthaltenen Anfälligkeiten verweisen. Das Extra nutzt zudem die erweiterten Paketbereitstellungsfunktionen von LANDesk, wie Targeted Multicast, Peer-Download und Checkpoint-Neustart, um Patches zügig und effizient bereitzustellen. Weitere Informationen zu diesen Softwareverteilungsfunktionen finden Sie unter "Softwareverteilung/Verteilungspakete/Verteilungsmethoden" auf Seite 269.

Reparieren von einer oder mehreren Definitionen gleichzeitig

Mit jeder der im Folgenden beschriebenen drei Behandlungsmethoden können Sie eine einzelne erkannte Definition oder eine Definitionsgruppe reparieren.

Um nacheinander Definition für Definition zu reparieren, klicken Sie mit der rechten Maustaste auf das Objekt und klicken dann auf **Reparieren**.

Um eine Gruppe von Definitionen in einem Arbeitsgang zu reparieren, kopieren Sie Definitionen aus einer der Inhaltsgruppen in eine benutzerdefinierte Gruppe (siehe "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584), klicken mit der rechten Maustaste auf die Gruppe und klicken dann auf **Reparieren**. Die Funktion "Automatisches Korrigieren" ist für benutzerdefinierte Gruppen allerdings nicht verfügbar. Sie können jedoch mehrere Definitionen in einer Liste auswählen, mit der rechten Maustaste darauf klicken und dann **Automatisches Korrigieren** wählen.

Reparatur von der Konsole aus

Wie oben beschrieben, können Windows- und Macintosh-Anfälligkeiten, benutzerdefinierte Definitionen, LANDesk Softwareupdates und blockierte Anwendungen von der Konsole aus repariert werden.

Die Reparatur mittels geplantem Task lässt sich mit einer Pushverteilung vergleichen, da das Patch vom Coreserver via Pushprozedur an Geräte übermittelt wird. Eine Richtlinie ist dagegen als Pullverteilung einzustufen, da der Richtlinienagent auf dem Gerät den Coreserver auf zutreffende Richtlinien durchsucht und das Patch dann mittels Pullprozedur vom Coreserver abruft.

Durchführen eines geplanten Reparaturtasks

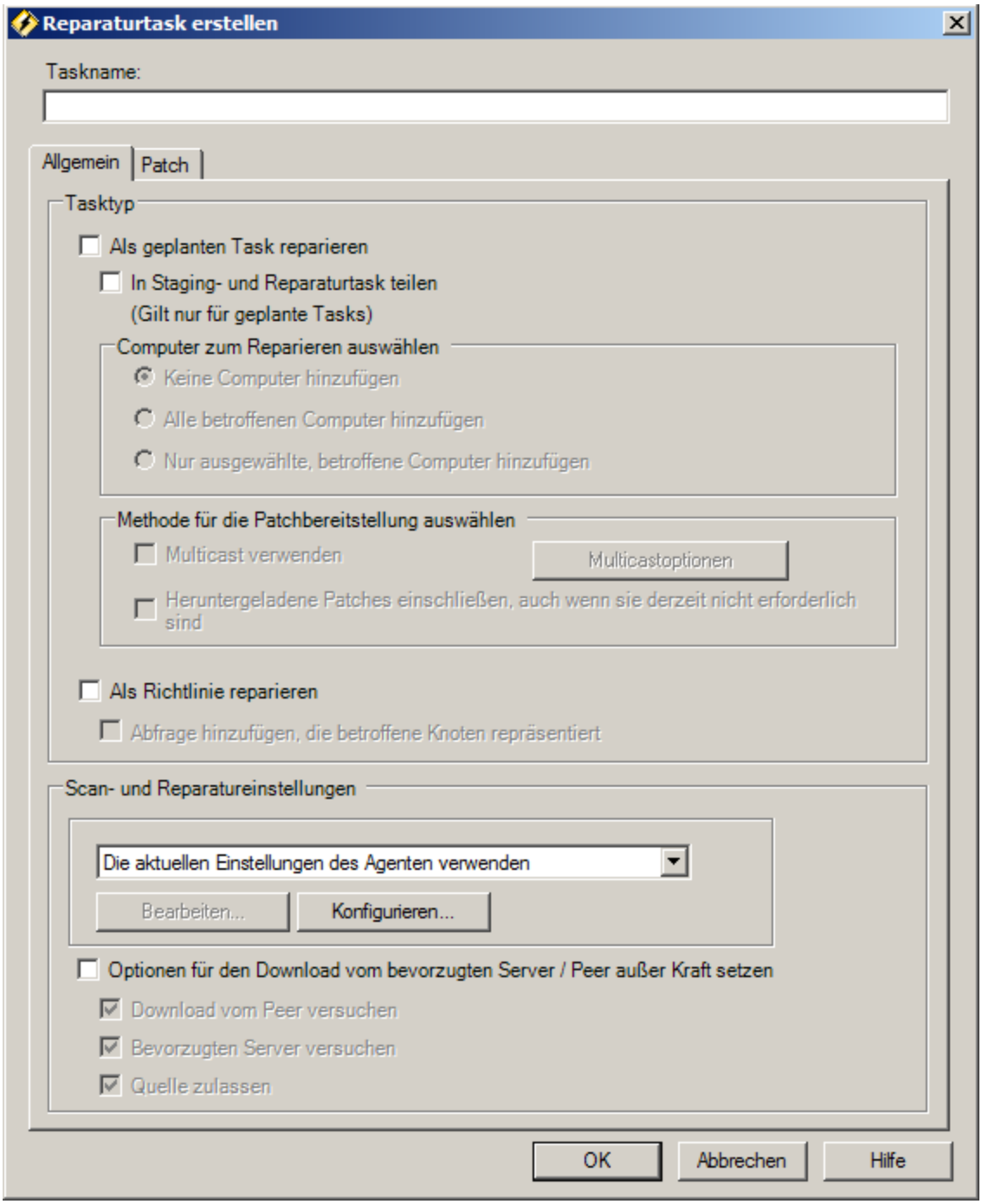
Das Planen eines Problembeseitigungs- oder Reparaturtasks ist sinnvoll, wenn Sie den Task so einrichten möchten, dass er zu einem bestimmten späteren Zeitpunkt oder als periodisch wiederkehrender Task ausgeführt werden soll. Patch und Compliance verwendet das Extra "Geplante Tasks", um einen geplanten Reparaturtask zu konfigurieren und zu bearbeiten.

Die Reparatur durch einen geplanten Task wird sowohl auf Windows- als auch auf Macintosh-Geräten unterstützt.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Sicherheitskonfigurationen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

So erstellen Sie einen geplanten Reparaturtask

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie mit der rechten Maustaste auf eine einzelne Definition in einer der Inhaltsgruppen oder klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Gruppe mit Definitionen, und klicken Sie dann auf **Reparieren**. Oder Sie können auf die Schaltfläche **Task erstellen** in der Symbolleiste und dann auf **Reparieren** klicken. Das Dialogfeld **Reparaturtask erstellen** wird angezeigt.



3. Bearbeiten Sie den **Tasknamen**, wenn Sie den Namen des Reparaturtasks ändern möchten.
4. Aktivieren Sie das Kontrollkästchen **Als geplanten Task reparieren**.
5. (Optional) Falls Sie diesen Reparaturtask in zwei Teile teilen möchten (einen Staging-Task, der die erforderlichen Patches auf den betroffenen Geräten bereitstellt, und den eigentlichen Reparaturtask, der das Patch installiert), klicken Sie auf **In Staging- und Reparaturtask teilen**.
6. Geben Sie an, welche Geräte Sie reparieren möchten. Wenn die aktuell betroffenen Geräte automatisch zur Zielliste im Fenster "Geplante Tasks" hinzugefügt werden sollen, aktivieren Sie das Kontrollkästchen **Alle betroffenen Geräte hinzufügen**. Mit anfälligen Geräten sind diejenigen Geräte gemeint, auf denen die Anfälligkeit während des letzten Scans erkannt wurde. Sobald der Task im Fenster "Geplante Tasks" erstellt wurde, können Sie weitere Ziele hinzufügen.
7. Falls Patches mittels Targeted Multicast verteilt werden sollen, aktivieren Sie das Kontrollkästchen **Multicast verwenden**. Zum Konfigurieren der Multicast-Optionen wählen Sie die Schaltfläche **Multicastoptionen**. Weitere Einzelheiten finden Sie unter "Informationen zum Dialogfeld "Multicastoptionen"" auf Seite 674.
8. Wenn Sie Peer-Download nur für die Patchbereitstellung verwenden möchten, aktivieren Sie das Kontrollkästchen **Patch nur von lokalen Peers downloaden**. Wenn diese Option ausgewählt ist, wird die Patchdatei nur verteilt, wenn sie sich entweder im lokalen Cache des Geräts befindet oder in einem Peer im selben Subnetz. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Patchinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sie sich an einem dieser beiden Orte befindet.
9. Geben Sie an, ob das Patch nur gedownloadet und nicht an betroffene Geräten verteilt und dort installiert werden soll.
10. Wählen Sie eine Scan- und Reparatureinstellung für diesen Reparaturtask aus. Scan- und Reparatureinstellungen definieren die Scanneranzeige, das Neustartverhalten, die Benutzerinteraktion auf gescannten Geräten sowie den eigentlichen gescannten Inhalt.
11. Klicken Sie auf **OK**.
12. Der Task wird im Fenster "Geplante Tasks" unter dem oben angegebenen Auftragsnamen angezeigt; in diesem Fenster können Sie Liste mit den Zielgeräten weiter anpassen und Planungsoptionen für den Auftrag konfigurieren.

Verwenden einer Reparaturrichtlinie (nur Windows)

Eine richtlinienbasierte Behandlung bietet Flexibilität, da Sie Zielgeräte (abhängig von den Ergebnissen einer benutzerdefinierten LDAP- oder Core-Datenbankabfrage) dynamisch festlegen können. Sie können beispielsweise eine Reparaturrichtlinie so konfigurieren, dass die Reparatur lediglich auf Geräten in einem bestimmten Verzeichnis-Container oder nur auf Geräten mit einem bestimmten Betriebssystem (oder einem anderen abfragbaren Inventarattribut) ausgeführt wird. Patch und Compliance verwendet Richtlinien im Extra "Geplante Tasks"/"Softwareverteilung", um Reparaturrichtlinien zu konfigurieren und zu verarbeiten.

HINWEIS: Unterstützte Plattformen für die richtlinienbasierte Reparatur
Die richtlinienbasierte Reparatur wird nur auf Windows-Geräten unterstützt. Macintosh-Geräte können nicht mit der Anwendungsrichtlinienmethode repariert werden.

Um von einer Richtlinie repariert zu werden, muss auf dem Gerät der Softwareverteilungsagent installiert sein. Wenn der Agent läuft, überprüft er die Coredatenbank auf das Vorhandensein von Richtlinien, die auf das Gerät zutreffen könnten. Sind solche Richtlinien vorhanden, wird auf dem Gerät ein Dialogfeld mit empfohlenen und optionalen Richtlinien (erforderliche Richtlinien, die automatisch angewendet werden) angezeigt.

Behandlungs- (oder Reparatur-)richtlinien funktionieren ganz ähnlich wie Anwendungsrichtlinien, abgesehen davon, dass Patchdateien statt Anwendungsdateien verteilt werden. Für Reparatur- und Anwendungsrichtlinien gelten im Grunde dieselben Voraussetzungen für die Richtlinienverwaltung, dieselben Bedingungen für den Taskablauf, dieselben Richtlinientypen und dieselben Bedingungen für die statische und dynamische Auswahl der Zielclients.

So erstellen Sie eine richtlinienbasierte Reparatur

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie mit der rechten Maustaste auf eine einzelne Definition in einer der Inhaltsgruppen oder klicken Sie mit der rechten Maustaste auf eine benutzerdefinierte Gruppe mit Definitionen, und klicken Sie dann auf **Reparieren**. Oder Sie können auf die Schaltfläche **Task erstellen** in der Symbolleiste und dann auf **Reparieren** klicken. Das Dialogfeld **Reparaturtask erstellen** wird angezeigt.
3. Bearbeiten Sie den **Tasknamen**, wenn Sie den Namen des Reparaturtasks ändern möchten.
4. Markieren Sie das Kontrollkästchen **Als Richtlinie reparieren**.
5. Wenn Sie basierend auf dieser Anfälligkeitsdefinition eine neue Abfrage erstellen möchten, mit der später andere verwaltete Geräte gescannt werden können, aktivieren Sie das Kontrollkästchen **Abfrage hinzufügen**.
6. Wenn Sie Peer-Download nur für die Patchbereitstellung verwenden möchten, aktivieren Sie das Kontrollkästchen **Patch nur von lokalen Peers downloaden**. Wenn diese Option ausgewählt ist, wird die Patchdatei nur verteilt, wenn sie sich entweder im lokalen Cache des Geräts befindet oder in einem Peer im selben Subnetz. Mit dieser Option lässt sich Netzwerkbandbreite sparen; die Patchinstallation kann aber nur dann erfolgreich ausgeführt werden, wenn sie sich an einem dieser beiden Orte befindet.
7. Geben Sie an, ob das Patch nur gedownloadet und nicht an betroffene Geräten verteilt und dort installiert werden soll.
8. Wählen Sie eine Scan- und Reparatureinstellung für diese Reparaturrichtlinie aus. Scan- und Reparatureinstellungen definieren die Scanneranzeige, das Neustartverhalten, die Benutzerinteraktion auf gescannten Geräten sowie den eigentlichen gescannten Inhalt.
9. Klicken Sie auf **OK**.
10. Die neue Richtlinie wird in der Gruppe "Richtlinien" im Fenster "Geplante Tasks" unter dem oben angegebenen Namen angezeigt. Hier können Sie jetzt statische Ziele (Benutzer oder Geräte) und dynamische Ziele (Abfrageergebnisse) hinzufügen sowie Typ und Häufigkeit der Richtlinie konfigurieren.

Durchführen einer Reparatur mithilfe von "Automatisches Korrigieren"

"Automatisches Korrigieren" ist eine einfach zu bedienende, integrierte Methode für die zügige Reparatur in Fällen, in denen Sie keinen geplanten Task oder keine Richtlinie zur Ausführung eines Reparaturtasks erstellen möchten. Wenn beispielsweise eine neue Anfälligkeit bekannt wird, die Sie in einem Schritt suchen und reparieren möchten, dann können Sie hierzu die Funktion "Automatisches Korrigieren" einsetzen.

"Automatisches Korrigieren" ist für folgende Inhalte verfügbar: Anfälligkeiten, Spyware, LANDesk Softwareupdates und benutzerdefinierte Definitionen.

WICHTIG: Voraussetzungen für den Einsatz der Funktion "Automatisches Korrigieren"
Nur Administratoren oder Benutzer, die das Patch Manager-Recht *und* den Bereich "Standardbereich: Alle Rechner" besitzen, können die Funktion "Automatisches Korrigieren" für die entsprechenden Definitionen aktivieren. LANDesk Benutzer, die weder das LANDesk Administrator- noch das Patch Manager-Recht besitzen, sehen diese Option noch nicht einmal im Kontextmenü einer Definition (das durch Klicken mit der rechten Maustaste geöffnet wird). Weitere Informationen zu Benutzerrechten und Bereichen finden Sie unter "Benutzerverwaltung" auf Seite 40.

Die Funktion "Automatisches Korrigieren" muss an zwei Stellen aktiviert sein, damit sie ordnungsgemäß funktioniert. Erstens muss die Option "Automatisches Korrigieren" eingeschaltet werden, und zweitens müssen die Scan- und Reparatureinstellungen auf den geplanten Scantask angewendet werden. Wenn die Funktion "Automatisches Korrigieren" für eines dieser beiden Elemente *nicht* aktiviert ist, funktioniert die automatische Korrektur nicht.

Wenn die Funktion "Automatisches Korrigieren" (wie oben beschrieben) an beiden Stellen aktiviert ist, dann verteilt und installiert Patch und Compliance automatisch das erforderliche Patch auf allen betroffenen Geräten, sobald der Sicherheitsscanner das nächste Mal ausgeführt wird (entweder manuell oder mittels Scantask). Wenn die Funktion "Automatisches Korrigieren" aktiviert ist und ein Patch einen Neustart erforderlich macht, wird das Zielgerät immer automatisch neu gestartet.

Sie können die Funktion "Automatisches Korrigieren" für eine einzelne Definition oder eine Gruppe mit mehreren Definitionen aktivieren.

So konfigurieren Sie eine Behandlung durch die Funktion "Automatisches Korrigieren"

1. Klicken Sie im Fenster des Extras **Patch und Compliance** mit der rechten Maustaste auf eine oder mehrere ausgewählte Definitionen aus den Inhaltsgruppen und klicken Sie dann auf **Automatisches Korrigieren beim Scannen**. (**HINWEIS:** Sie können die Funktion "Automatisches Korrigieren" nicht für eine benutzerdefinierte Gruppe aktivieren.)
2. Führen Sie den Sicherheitsscanner auf den zu scannenden Geräten aus und eine automatische Reparatur, indem Sie einen geplanten Sicherheitsscan-Task mit einer Scan- und Reparatureinstellung ausführen, bei dem die Option "Automatisches Korrigieren" aktiviert ist.

Manuelles Reparieren von Linux- und UNIX-Geräten

Unterstützte Windows- und Mac-Geräte können von der Konsole ferngesteuert repariert werden. Andere Plattformen wie Linux und UNIX Sun Solaris hingegen, können von der Konsole aus nur gescannt, aber nicht repariert werden.

Sie müssen die entsprechenden Patches manuell auf Linux- und UNIX-Geräten installieren, um sie zu reparieren.

Was passiert auf einem Gerät während des Reparaturvorgangs?

Eine automatische Reparatur umfasst die Verteilung und Installation von Patches auf verwalteten Geräten, wobei jede der drei in den vorhergehenden Abschnitten beschriebenen Methoden eingesetzt werden kann.

Denken Sie stets daran, dass ein Reparaturauftrag das Korrigieren einer oder mehrerer erkannter Sicherheitsdefinitionen beinhalten kann. Zudem ist zu beachten, dass die Reparatur einer erkannten Definition die Installation eines oder mehrerer Patches erfordern kann. Wegen dieser Faktoren kann die Reparatur, abhängig von Anzahl und Typ der Erkennungen, zur Folge haben, dass auf dem Gerät nur eine Patchdatei installiert wird oder dass mehrere Patchdateien auf dem Gerät installiert werden.

Fast alle Patchdateien können unbeaufsichtigt (transparent) installiert werden, wobei keine Benutzereingriffe am Endanwendergerät erforderlich sind. Die Installation einiger Windows 9.x-Patches und Patches für andere Sprachen als Englisch erfordern Benutzereingriffe. Ob ein Patch unbeaufsichtigt installiert werden kann, können Sie der Spalte "Unbeaufsichtigte Installation" in einer der Patchlisten entnehmen. Weitere Informationen finden Sie unter "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584.

Konfigurieren der Sicherheitsscanner-Anzeige und Interaktion auf Endanwendergeräten

Unabhängig davon, ob eine Patchdatei unbeaufsichtigt installiert werden kann oder nicht, können Sie jetzt mit der Funktion zum Konfigurieren der Scan- und Reparatureinstellungen festlegen, wie viel der Sicherheitsscanner auf dem Endanwendergerät anzeigen und wie viele Abfragen er einblenden soll.

HINWEIS: Konsolidierter Neustart
Wenn die Installation einer Patchdatei einen Neustart erforderlich macht (*und* die Option **Nie neu starten** auf der Seite "Neu starten" der für diesen Task geltenden Scan- und Reparatureinstellungen nicht ausgewählt ist), installiert Patch und Compliance zuerst *alle* Patches des angegebenen Tasks auf dem Gerät und startet dann das Gerät einmal neu.

Zusätzliche Befehle (nur für benutzerdefinierte Definitionen)

Die Reparatur einer benutzerdefinierten Reparatur kann nach Bedarf zusätzliche Sonderbefehle einschließen, die während der Erstellung einer benutzerdefinierten Erkennungsregel definiert werden. Zusätzliche Befehle werden in der Reihenfolge ausgeführt, die auf der Registerkarte "Befehle" für die betreffende Regel festgelegt wurde und mit den Argumenten eines jeden Befehls übereinstimmt. Zusätzliche Befehle können bevor, nachdem und während die eigentliche Patchdatei ausgeführt wird, ausgeführt werden.

Anzeigen von Patch- und Compliance-Informationen für gescannte Geräte

Wie weiter oben beschrieben, lassen sich gescannte Sicherheitsdaten u.a. nach Gerät sortiert anzeigen. Klicken Sie hierfür mit der rechten Maustaste auf ein einzelnes Gerät oder eine Gruppe ausgewählter Geräte und klicken Sie dann auf **Sicherheits- und Patchinformationen**.

Diese Seite enthält zahlreiche nützliche Funktionen. Wenn Sie ein oder mehrere Geräte ausgewählt haben, können Sie Folgendes tun:

- Anzeigen von Listen mit erkannten Definitionen
- Anzeigen, wann und warum die Erkennung erfolgte
- Anzeigen von Listen mit installierten Patches und Softwareupdates
- Anzeigen, wann das Patch installiert oder deinstalliert wurde
- Löschen des Patch-Installationsstatus
- Anzeigen von Daten zum Reparaturverlauf
- Löschen von Daten zum Reparaturverlauf

Sie können auch mit der rechten Maustaste auf Definitionen und Erkennungsregeln in den entsprechenden Elementlisten klicken, um globale Tasks auf einem oder mehreren betroffenen Geräten auszuführen.

Anzeigen der letzten Sicherheitsscandaten im Geräteinventar

Um nachzuprüfen, wann der letzte Sicherheitsscan auf einem Gerät ausgeführt wurde, klicken Sie mit der rechten Maustaste auf das Gerät, klicken auf **Inventar** und blättern dann mit der Bildlaufleiste nach unten zu den verschiedenen Einträgen **Datum des letzten Scans** im rechten Fensterausschnitt der Inventaransicht.

Überprüfen des Reparaturstatus

Nachdem die Reparatur auf den betroffenen Geräten durchgeführt wurde, gibt Patch und Compliance Statusinformationen zur jeweiligen Patchinstallation aus. Sie können den Status der Patchinstallation nach Anfälligkeit/Definition oder nach Zielgeräten getrennt überprüfen.

So überprüfen Sie eine Patchinstallation auf einem Gerät

1. Führen Sie den Sicherheitsscanner auf dem Gerät aus.
2. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf ein repariertes Gerät und klicken Sie dann auf **Sicherheits- und Patchinformationen**.
3. Klicken Sie im linken Fensterausschnitt auf das Objekt **Installierte Patches**.
4. Wählen Sie die Felder **Patchinformationen** am unteren Rand des Dialogfelds.

Das Feld **Installationsstatus** gibt an, ob die Installation erfolgreich war. Folgende Statuswerte sind möglich: "Erfolgreich", "Fehlgeschlagen" und "Fehler beim Downloaden".

Löschen des Anfälligkeitsscan- und Reparaturstatus nach Anfälligkeit

Falls die Patchinstallation misslungen ist, müssen Sie zuerst die den Installationsstatus betreffenden Informationen löschen, bevor Sie erneut versuchen, das Patch zu installieren. Sie können die Installations-/Reparaturstatusinformationen für das betroffene Gerät löschen, indem Sie im Dialogfeld **Sicherheits- und Patchinformationen** auf **Löschen** klicken. Sie können außerdem den Patchinstallationsstatus nach Anfälligkeit löschen.

Sie können Anfälligkeitsscan- und Reparaturstatusinformationen für alle von einer Anfälligkeit (oder mehreren Anfälligkeiten) betroffenen Geräte mithilfe des Dialogfelds **Scan- bzw. Reparaturstatus löschen** entfernen. Wenn eine Patchinstallation misslingt, müssen Sie (wie oben beschrieben) zuerst den Installationsstatus (Reparaturstatus) löschen, bevor Sie erneut versuchen, das Patch zu installieren.

Sie können mit diesem Dialogfeld auch Anfälligkeitsscan-Informationen für eine oder mehrere Anfälligkeiten aus der Datenbank löschen.

So löschen Sie den Anfälligkeitsscan- und Reparaturstatus

1. Klicken Sie mit der rechten Maustaste auf die Anfälligkeit und wählen Sie dann **Scan- bzw. Reparaturstatus löschen** aus.
2. Wählen Sie die gewünschten Optionen aus.
3. Klicken Sie auf **OK**.

Erstellen eines geplanten Neustarttasks

Patch und Compliance stellt ein Extra bereit, mit dem Sie einen Task für einen Geräteneustart erstellen können. Ein Neustarttask ist eine nützliche Funktion, wenn Sie Patches (ohne Neustart) als einzelnen Prozess installieren und dann die auf diese Weise reparierten Geräte in einem separaten Task neu starten möchten. Beispiel: Sie können einen Scan- oder Patchinstallationstask tagsüber und dann einen reinen Neustarttask zu einer für die Endbenutzer günstigeren Uhrzeit ausführen lassen.

So erstellen Sie einen Neustart-Task

1. Klicken Sie auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Neu starten**.
3. Geben Sie an, ob der Neustart ein geplanter Task, ein richtlinienbasierter Scan oder beides ist.
4. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste der verfügbaren Einstellungen aus (oder erstellen Sie eine benutzerdefinierte Einstellung speziell für diesen Scantask), um anzugeben, wie der Scanner auf Endanwendergeräten ausgeführt wird. (**HINWEIS:** Nur die Neustarteinstellungen in der Scan- und Reparatureinstellungen werden bei einem Neustarttask verwendet.)
5. Klicken Sie auf **OK**. Für einen geplanten Task können Sie jetzt Zielgeräte hinzufügen und die Zeitplanoptionen im Extra "Geplante Tasks" konfigurieren. Bei einer Richtlinie wird die neue Richtlinie im Fenster "Application Policy Management" unter dem oben angegebenen Tasknamen angezeigt. Hier können Sie jetzt statische Ziele (Benutzer oder Geräte) und dynamische Ziele (Abfrageergebnisse) hinzufügen sowie Typ und Häufigkeit der Richtlinie konfigurieren.

Verwenden der Sicherheitsscanner-Befehlszeile

Das Extra "Patch und Compliance" bildet die wichtigste Komponente der umfassenden Sicherheitsverwaltungslösung von LANDesk Security Suite. Dieses Extra verwenden Sie zum Downloaden von Updates für Definitionen und Patches verschiedener Sicherheitsinhaltstypen sowie zum Erstellen, Konfigurieren und Ausführen von Sicherheitsanalysescans, Compliance- und Reparaturscans, Aktivieren von Sicherheitsalarmen, Generieren von Sicherheitsberichten und mehr. Weitere Informationen finden Sie unter "Patch und Compliance" auf Seite 578 und unter "Hilfe zu Patch und Compliance" auf Seite 652.

Dieser Abschnitt stellt zusätzliche Informationen zur Verwendung des Patch- und Compliance-Sicherheitsscanners bereit.

Befehlszeilenparameter für den Sicherheitsscanner

Der Sicherheitsscanner heißt vulscan.exe. Der Scanner unterstützt die folgenden Befehlszeilenparameter:

Parametername	Beschreibung
Allgemeine Parameter	
/AgentBehavior=ScanRepairSettingsID	Überschreibt das Verhalten des Sicherheitsscanners (Scan- und Reparatureinstellungen) nur für die aktuelle Sicherheitsbewertung oder den aktuellen Remediation-Scanjob. Die ScanRepairSettings-ID ist ein Zahlenwert.

Parametername	Beschreibung
/ChangeBehaviors /AgentBehavior=ScanRepairSettingsID	Ändert die Standard-Scan- und Reparatureinstellungen für alle nachfolgenden Sicherheitsbewertungen oder Remediation-Scanjobs, indem die Scan- und Reparatureinstellungen in die lokale Registrierung des Geräts geschrieben werden. Verwenden Sie die exakte Syntax auf der linken Seite, mit beiden Switches in der Befehlszeile. Die ScanRepairSettings-ID ist ein Zahlenwert. **HINWEIS:** Sie können diese Option verwenden, um die Standard-Scan- und Reparatureinstellungen für ein Gerät zu ändern, ohne eine vollständige Agentenkonfiguration auf dem Gerät bereitstellen zu müssen.
/ShowUI	Zeigt die Scanner-Benutzeroberfläche auf dem Endbenutzergerät.
/AllowUserCancelScan	Zeigt eine Schaltfläche zum Abbrechen auf der Scanner-Benutzeroberfläche an, mit der der Endbenutzer den Scan beenden kann.
/AutoCloseTimeout=Number	Zeitüberschreitungswert in Sekunden. **HINWEIS:** Falls der Wert auf -1 eingestellt ist, wartet die Scanner-Benutzeroberfläche darauf, vom Endbenutzer manuell geschlossen zu werden.
/Scan=Number Code (0-8)	Gibt an, nach welchem Sicherheitsinhaltstyp gesucht wird. Die Zahlencodes für die verschiedenen Sicherheitsinhaltstypen sind: 0 - Anfälligkeit 1 - Spyware 2 - Sicherheitsbedrohung 3 - LANDesk Updates 4 - benutzerdefinierte Definition 5 - blockierte Anwendung 6 - Softwareupdates 7 - Treiberupdates 8 - Virenschutz 100 - alle Typen

Parametername	Beschreibung
/Group=GroupID	Identifiziert die Sicherheitsinhaltsgruppe, nach der gescannt wird. Diese Option überschreibt spezifische Inhaltstyp-Parameter, sofern vorhanden.
/AutoFix=True or False	Aktiviert oder deaktiviert die automatische Reparaturfunktion.
Reparaturparameter	
/Repair (Group=GroupID, or Vulnerability=VulnerabilityID, or Vulnerability=All)	Teilt dem Scanner mit, welche Gruppe oder Anfälligkeit repariert werden soll. Sie können "Alle" für Anfälligkeiten angeben; damit werden anstatt einer einzelnen Anfälligkeit anhand ihrer ID alle erkannten Anfälligkeiten repariert.
/RemovePatch=PatchName	Entfernt das angegebene Patch aus dem Patchrepository.
/RepairPrompt=MessageText	Hiermit können Sie eine Textmeldung anzeigen, die den Endbenutzer zur Eingabe auffordert.
/AllowUserCancelRepair	Eine Zeichenfolge, die dem Endbenutzer das Abbrechen der Reparatur erlaubt, falls eine Reparatureingabeaufforderung verwendet wird.
/AutoRepairTimeout=Number	Ein Timeoutwert für die Reparatureingabeaufforderung in Sekunden. Falls dieser Wert auf -1 eingestellt ist, wartet die Eingabeaufforderung darauf, vom Benutzer manuell geschlossen zu werden.
/DefaultRepairTimeoutAction	Eine Zeichenfolge für die von vulscan zu initiierende Standardaktion, wenn der Timeout für Reparatureingabeaufforderungen abläuft. Zu den zulässigen Werte gehören "start" und "close".
/StageOnly	Eine Zeichenfolge zum Abrufen des Patches bzw. der Patches, die zur Reparatur benötigt jedoch nicht installiert werden.
/Local (Dateien vom Peer abrufen)	Erzwingt reinen Peer-Download.
/PeerDownload	Entspricht /local.
/SadBandwidth=Number	Maximal zulässige Bandbreite (in Prozent) beim Downloaden.
Neustartparameter	

Parametername	Beschreibung
/RebootIfNeeded	Verwenden Sie diesen Parameter ggf. zum Neustart eines Computers.
/RebootAction	Eine Zeichenfolge, die das Neustartverhalten von vulscan bei der Reparatur bestimmt. Zulässige Werte sind: "always" (immer),"never" (nie) und "empty" (leer) bzw. "anthing else" (alles andere). Falls "anything else", dann führt vulscan bei Bedarf den Neustart aus.
/RebootMessage	Eine Zeichenfolge, die auf dem Bildschirm des Endbenutzers eine Textmeldung in einer Neustart-Eingabeaufforderung anzeigt.
/AllowUserCancelReboot	Eine Zeichenfolge, die dem Endbenutzer das Abbrechen des Neustarts gestattet, falls eine Neustart-Eingabeaufforderung verwendet wird.
/AutoRebootTimeout=Number	Timeoutwert für ein Reparatureingabeaufforderung in Sekunden. Falls dieser Wert auf -1 eingestellt ist, wartet die UI darauf, vom Benutzer manuell geschlossen zu werden.
/DefaultRebootTimeoutAction	Eine Zeichenfolge, mit der festgelegt wird, welche Aktion vulscan ausführt, falls der Timeoutwert für die Neustart-Eingabeaufforderung abläuft. Zulässige Werte sind: "reboot" (neu starten), "close" (schließen), "snooze" (erneut erinnern).
/SnoozeCount=Number	Erneute Erinnerungen: Anzahl der Verzögerungen, die vulscan immer dann anpasst, wenn der Benutzer in der Neustart-Eingabeaufforderung auf **Snooze** klickt.
/SnoozeInterval=Number	Anzahl der Sekunden, die vulscan zwischen "Snoozes" ruht.
MSI-Parameter	
/OriginalMSILocation=path	Pfad zum ursprünglichen MSI-Speicherort.
/Username=Benutzername	Benutzername für das MSI-Verzeichnis.
/Password=Kennwort	Kennwort für das MSI-Verzeichnis.
Deaktivierungsparameter	
/NoElevate	Vulscan nicht über Core-Tech starten.

Parametername	Beschreibung
/NoSleep	Verhindert Ruhephasen während des Definitionsscans.
/NoSync	Kein mutex, scannt mehrere Instanzen.
/NoUpdate	Keine neue Version von vulscan abrufen.
/NoXML	msxml nicht suchen.
/NoRepair	Wie autofix=false. Überschreibt die Einstellungen für "Automatisches Korrigieren", falls vorhanden.
Datendateiparameter	
/Dump	Anfälligkeitsdaten direkt vom Webdienst speichern.
/Data	Nimmt Anfälligkeitsdaten auf (von /dump).
/O=Path\Filename	Gibt Scanergebnisse aus.
/I=Path\Filename	Gibt Scanergebnisse ein.
/Log=Path\Filename	Überschreibt den Protokolldateinamen.
/CoreServer=Servername	Identifiziert den Coreserver-Namen.
/Reset	Entfernt Delta-Datei-Basisinformationen (löscht das Anwendungsdatenverzeichnis).
/Clear oder /ClearScanStatus	Löscht alle Informationen zum Anfälligkeitsscan.

Konfigurieren von Patch und Compliance-Alarmen

Im folgenden Abschnitt werden andere Tasks beschrieben, die Sie mit dem Extra "Patch und Compliance" ausführen können.

Konfigurieren von Patch und Compliance-Alarmen

Sie können Sicherheitsalarme für Patch und Compliance konfigurieren, damit Sie beim Erkennen bestimmter Anfälligkeiten auf verwalteten Geräten in Ihrem System benachrichtigt werden. Die Funktion "Anfälligkeitsalarme" in Patch und Compliance verwendet das Standard-Alarmtool von LANDesk.

Eine Anfälligkeit muss in die Gruppe "Alarm" kopiert werden, damit bei ihrer Erkennung ein Alarm generiert wird. Eine Anfälligkeit in der Gruppe "Alarm" ist eine Kopie eines Alarms, der auch in der Gruppe "Scannen" enthalten ist. Nachdem Sie die gewünschten Anfälligkeitsdefinitionen in die Gruppe "Alarm" eingefügt haben (entweder manuell oder durch Angabe des Schweregrads von Anfälligkeiten, um diese beim Download automatisch zu platzieren), können Sie das Alarmintervall im Dialogfeld "Alarme konfigurieren" festlegen.

So konfigurieren Sie Alarme

1. Geben Sie an, welche Anfälligkeiten einen Alarm generieren, indem Sie gedownloadete Alarmdefinitionen in die Gruppe "Alarm" einfügen.
2. Oder klicken Sie auf die Symbolleistenschaltfläche **Einstellungen konfigurieren** und klicken Sie dann auf **Alarmeinstellungen**.
3. Geben Sie ein Mindestalarmintervall für die Alarmierung an.
4. Zum Konfigurieren der Sicherheitsalarmierung wählen Sie die Definitionen (nach Sicherheitsstufe) aus, für die Sie veranlassen möchten, dass sie während des Downloads automatisch in die Gruppe **Alarm** eingefügt werden. Sie können mehrere Schweregradstufen für Anfälligkeiten auswählen. Diese Anfälligkeitsdefinitionen werden auch automatisch in die Gruppe "Scannen" eingefügt.
5. Wenn Sie ein Antivirus-Alarmierung konfigurieren möchten, wählen Sie die Antivirus-Ereignisse aus, die einen Alarm auslösen sollen.
6. Klicken Sie auf **OK**.

Generieren von Patch und Compliance-Berichten

Die Patch- und Compliance-Informationen werden in mehreren Berichten im Extra "Berichte" dargestellt. Diese Berichte stellen für alle der verschiedenen Sicherheitsrisiko-Inhaltstypen ein breites Spektrum an nützlichen Informationen zur Bewertung des Sicherheitsrisikos, zu Compliance, zu Patchbereitstellung und zum Reparaturstatus für verwaltete Geräte in Ihrem Netzwerk zur Verfügung.

Um auf das Extra "Berichte" zugreifen und Berichte generieren und anzeigen zu können, müssen Benutzer über das Recht "LANDesk Administrator" (d. h. uneingeschränkte Rechte) und die spezifischen Rollen für "Berichte" verfügen.

Weitere Informationen zur Verwendung des Extras "Berichte" finden Sie unter "Berichte" auf Seite 209.

Compliance mit den FDCC-Standards – Übersicht

LANDesk Security Suite bietet jetzt erweiterte Unterstützung für Sicherheitsscans und Reparaturen gemäß der Federal Desktop Core Configuration (FDCC)-Initiative. Infolgedessen wurden LANDesk Softwareprodukte offiziell vom National Institute of Standards and Technology (NIST) als mit den Security Content Automation Protocol (SCAP)-Standards konform zertifiziert und sind als validierte Produkte auf der Website "National Vulnerability Database" aufgeführt.

Compliance mit den FDCC-Standards können Sie für die Netzwerkumgebung Ihres Unternehmens einführen, indem Sie die Patch- und Compliance-Extras und -Funktionen verwenden, um grundlegende Sicherheitsscan- und Reparaturtasks mit FDCC-zertifiziertem Sicherheitsinhalt (d. h. Anfälligkeitsdefinitionen) durchzuführen. Mit einem Sicherheitsinhalts-Abonnement, das diesen von LANDesk veröffentlichten FDCC-zertifizierten Sicherheitsinhalt umfasst, können Sie die FDCC-Sicherheitsscanner-Anwendung erkennen und installieren, die Compliance mit den FDCC-Sicherheitsstandards überprüfen und FDCC-Anfälligkeitsscans und Reparaturen ausführen. Auf diese Weise stellen Sie sicher, dass Ihre verwalteten Geräte (Clients) die Standards und Anforderungen laut Federal Desktop Core Configuration-Initiative erfüllen.

Validierte SCAP-Funktionalitäten

Die folgenden Funktionalitäten für Anfälligkeitsscans, Patchmanagement und Reparatur (laut Definition des National Institute of Standards and Technology, NIST) wurden für LANDesk Security Suite validiert:

- **FDCC-Scanner:** "Die Funktionalität zur Überprüfung und Bewertung eines Zielsystems, um dessen Konformität mit den FDCC-Anforderungen zu bestimmen."
- **Authentifizierter Konfigurationsscanner:** "Die Funktionalität zur Überprüfung und Bewertung eines Zielsystems, um dessen Konformität mit einem definierten Satz von Konfigurationsanforderungen unter Verwendung von Systemanmeldeprivilegien zu bestimmen."
- **Authentifizierter Anfälligkeits- und Patchscanner:** "Die Funktionalität zum Scannen eines Zielsystems zwecks Lokalisierung und Identifizierung des Vorhandenseins bekannter Anfälligkeiten und Bewertung des Softwarepatchstatus, um die Konformität mit einer definierten Patchrichtlinie unter Verwendung von Systemanmeldeprivilegien zu bestimmen."

Unterstützte Geräteplattformen

FDCC-zertifizierte Anfälligkeitsscans und Reparaturen von Anfälligkeiten werden auf folgenden Plattformen für verwaltete Geräts (Clients) unterstützt.

- Microsoft Windows Vista SP1
- Microsoft Windows XP Professional SP3

Download von FDCC-spezifischem Sicherheitsinhalt

Dieser Abschnitt enthält schrittweise Anleitungen für den Download von Federal Desktop Core Configuration (FDCC)-spezifischem Sicherheitsinhalt.

WICHTIG: Denken Sie daran, dass Sie ein Inhaltsabonnement gezeichnet haben müssen, damit Sie Sicherheitsinhalte herunterladen können. In diesem Fall müssen Sie ein LANDesk Security Suite Inhaltsabonnement haben, das explizit den FDCC-Inhalt einschließt.

So laden den FDCC-Sicherheitsinhalt herunter

1. Klicken Sie in der Konsole auf **Extras > Sicherheit > Patch und Compliance**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Updates downloaden**.
3. Wählen Sie die Website für die Updatequelle in der Liste der verfügbaren Content-Server aus.
4. Wählen Sie die Definitionstypen aus, deren Sicherheitsinhalt Sie aktualisieren möchten. In diesem Fall wählen Sie in der Liste mit den Definitionstypen **Federal Desktop Core Configuration** aus. Sie können einen oder mehrere Typen aus der Liste auswählen (je nach LANDesk Security Suite-Inhaltsabonnement). Je mehr Typen Sie auswählen, umso länger dauert die Aktualisierung.
5. Wählen Sie die Sprachen aus, deren Inhalt Sie für die von Ihnen angegebenen Typen aktualisieren möchten. In diesem Fall wählen Sie **Englisch**.
6. Wenn Sie veranlassen möchten, dass neuer Inhalt (d. h. Inhalt, der noch nicht in einer der Gruppen existiert) automatisch in die Gruppe "Nicht zugewiesen" eingefügt wird, anstatt in den Standardspeicherort (die Gruppe "Scannen"), aktivieren Sie das Kontrollkästchen **Neue Definitionen in die Gruppe "Nicht zugewiesen" einfügen**.
7. Wenn Sie verknüpfte ausführbare Patchdateien automatisch herunterladen möchten, aktivieren Sie das Kontrollkästchen **Patches downloaden** und klicken anschließend auf eine der folgenden Downloadoptionen. (**HINWEIS:** Die Patches werden in den Speicherort heruntergeladen, der auf der Seite "Patchspeicherort" des Dialogfelds "Updates downloaden" angegeben wurde.

8. Wenn Ihr Netzwerk über einen Proxyserver verfügt, der für externe Internet-Übertragungen verwendet wird (für die Aktualisierung von Sicherheitsinhalten und den Download von Patches erforderlich), klicken Sie auf die Registerkarte **Proxyeinstellungen** und geben die Serveradresse, Portnummer sowie Anmeldeinformationen ein, wenn für den Zugriff auf den Proxyserver eine Anmeldung erforderlich ist.
9. Klicken Sie auf **Übernehmen**, wenn Sie die Einstellungen speichern möchten.
10. Klicken Sie auf **Jetzt aktualisieren**, um das Update für die Sicherheitsinhalte auszuführen. Das Dialogfeld "Definitionen werden aktualisiert" zeigt den aktuellen Vorgang und Status an.
11. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Schließen**. Wenn Sie auf **Abbrechen** klicken, bevor die Aktualisierung abgeschlossen ist, werden nur die bis zu diesem Zeitpunkt verarbeiteten Sicherheitsinhalte in die Coredatenbank heruntergeladen. Sie müssen die Aktualisierung erneut ausführen, um den restlichen Sicherheitsinhalt abzurufen.

Nachdem der Download des FDCC-Inhalts abgeschlossen ist, können Sie den Inhalt anzeigen und verwalten, um Compliancescans und Reparaturen durchzuführen.

Anzeigen von heruntergeladenen FDCC-Sicherheitsinhalten

Der FDCC-Inhalt wird auf den Coreserver heruntergeladen und unter dem übergeordneten Objekt "Vordefinierte Gruppen" wird eine neue Federal Desktop Core Configuration-Gruppe erstellt, die Untergruppen für unterstützte Betriebssystemplattformen (Windows Vista und Windows XP) sowie bestimmte Komponentenprüfungen enthält. Die Untergruppen der "Komponentenprüfung" sind folgende:

- Firewall
- Internet Explorer
- Patches
- Einstellungen

Die heruntergeladenen FDCC-Anfälligkeitsdefinitionen werden als Sicherheitsbedrohungen eingestuft. Wenn Sie die Definitionen anzeigen möchten, müssen Sie in der Dropdownliste "Typ" entweder **Sicherheitsbedrohungen** oder **Alle Typen** auswählen.

Installieren des FDCC-Sicherheitsscanners

Dieser Abschnitt beschreibt, wie verwaltete Geräte auf den FDCC-Sicherheitsscanner-Agenten bzw. die FDCC-Sicherheitsscanner-Anwendung überprüft und gegebenenfalls der Scanner installiert wird.

Nachdem Sie den FDCC-spezifischen Sicherheitsinhalt heruntergeladen haben, müssen Sie die FDCC-Scanneranwendung auf den verwalteten Geräten installieren. Erst dann können Sie FDCC-Anfälligkeitsbewertungsscans konfigurieren und ausführen.

Um den FDCC-Scanner auf Clients zu installieren, erstellen Sie einen geplanten Task zum Scannen und Reparieren der FDCC SCANNER INST ALL-Anfälligkeitsdefinition. Diese Definition findet sich in der Untergruppe **(Step 1) Install Scanner** der Gruppe **Federal Desktop Core Configuration**. Diese Definition für Sicherheitsbedrohungen prüft, ob der FDCC-Scanner auf Zielclients installiert werden muss. Wird die FDCC-Scanneranwendung nicht auf dem Client gefunden, besteht die Reparatur in der Installation der erforderlichen Verzeichnisse und Dateien. (**HINWEIS:** Die FDCC-Scanneranwendung wird in folgendem Verzeichnis installiert: \Programme\LANDesk\LDClient\S-CAT.)

WICHTIG: Die Gruppenberechtigung "LANDesk Script Writers" ist erforderlich, um diese Tasks auszuführen. Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Sicherheitskonfigurationen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Rollenbasierte Administration" im Benutzerhandbuch.

So erstellen Sie einen geplanten Task, der den FDCC-Scanner installiert

1. Klicken Sie in der Konsole auf **Extras > Sicherheit > Patch und Compliance**.
2. Stellen Sie sicher, dass der FDCC-Sicherheitsinhalt kürzlich aktualisiert wurde.
3. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitsscan**. Das Dialogfeld "Sicherheitsscantask erstellen" wird geöffnet.
4. Geben Sie einen Namen für den Scan ein.
5. Aktivieren Sie das Kontrollkästchen **Geplanten Task erstellen**.
6. Für die Erstellung von Scan- und Reparatureinstellungen, die die vordefinierte FDCC SCANNER-INSTALL-Definition für Sicherheitsbedrohungen verwenden, die in der Untergruppe "Install Scanner" als Inhalt für den Sicherheitsscan zu finden ist, klicken Sie auf **Konfigurieren** und anschließend auf die Seite **Scanoptionen**.
7. Um anzugeben, nach was gescannt werden soll, klicken Sie auf **Gruppe**. Klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie die Untergruppe **(Step 1) Install Scanner** der Gruppe **Federal Desktop Core Configuration**.
8. Geben Sie bei Bedarf auf den anderen Seiten mit Scan- und Reparatureinstellungen weitere Sicherheitsscanoptionen an.
9. Klicken Sie auf Speichern, um die Scan- und Reparatureinstellungen zu speichern, die Sie für diesen Scantask anwenden.
10. Klicken Sie beim Dialogfeld zum Sicherheitsscantask auf **OK**. Für einen Scan, der als geplanter Task ausgeführt wird, können Sie jetzt Zielgeräte hinzufügen und die Zeitplanoptionen im Extra "Geplante Tasks" konfigurieren.

Wenn Sie den Scan mit dieser Sicherheitsbedrohung ausführen, werden auf allen Zielgeräten, auf denen der FDCC-Scanner noch nicht installiert ist, die erforderlichen Anwendungsdateien installiert, wie oben ausgeführt. An diesem Punkt können Sie nun mit der FDCC-Complianceprüfung beginnen und Scans und Reparaturen mit FDCC-spezifischen Sicherheitsinhalten ausführen.

Überprüfen auf FDCC-Compliance

Dieser Abschnitt bietet Informationen zum Ausführen eines Sicherheitsscans auf Zielgeräten, auf dessen Basis ein FDCC-Compliance-Bericht generiert wird.

Sobald die FDCC-Scanneranwendung auf Ihren verwalteten Geräten Installiert ist, können Sie einen weiteren geplanten Sicherheitsscantask ausführen, der die Sicherheitsbedrohungsdefinition der ComplianceResultsFile verwendet. Diese Definition findet sich in der Untergruppe **(Step 2) Results File Scan** der Gruppe **Federal Desktop Core Configuration** und generiert die FDCC-Berichtsdaten. Finden sich keine Berichtsdaten auf dem Client oder sollten die Berichtsdaten älter sein, als die in der benutzerdefinierten Variablen angegebene Anzahl der Tage, wird die Sicherheitsbedrohungsdefinition erkannt, d. h. das Gerät ist nicht konform bzw. nicht "compliant".

Zur Erstellung eines Sicherheitsscantasks, der eine Überprüfung auf das Vorhandensein von FDCC-Berichtsdaten vornimmt und FDCC-Berichtsdaten generiert, führen Sie dieselben Schritte aus, wie oben unter **So erstellen Sie einen geplanten Sicherheitsscantask** beschrieben, wobei Sie in den Scan- und Reparatureinstellungen die Untergruppe **(Step 2) Results File Scan** als die Gruppe auswählen, nach der gescannt werden soll.

Ausführen von FDCC-Sicherheitsscans

Dieser Abschnitt beschreibt, wie FDCC-spezifischer Inhalt (Anfälligkeitsdefinitionen) zum Scannen und Reparieren von Sicherheitsrisiken auf Ihren verwalteten Geräten eingesetzt wird.

Jede FDCC-Untergruppe enthält Anfälligkeitsdefinitionen in Bezug auf Sicherheitsbedrohungen für jede der folgenden Komponenten:

- Firewall
- Internet Explorer
- Patches
- Einstellungen

Sie können diese Anfälligkeitsdefinitionen zur Erstellung geplanter Scantasks verwenden, die den Status "In Ordnung/Fehlgeschlagen" für jeden dieser FDCC-Sicherheitsbereiche prüfen. Diese Anfälligkeiten in Bezug auf Sicherheitsbedrohungen zeigen an, was auf Zielgeräten erkannt (d. h. als "Fehlgeschlagen" verzeichnet) wurde.

Zur Erstellung von Sicherheitsscantasks, die eine Überprüfung auf das Vorhandensein von komponentenspezifischen FDCC-Sicherheitsinhalten vornehmen, führen Sie dieselben Schritte aus, wie unter **So erstellen Sie einen geplanten Sicherheitsscantask** beschrieben, wobei Sie in den Scan- und Reparatureinstellungen die entsprechende Komponentenuntergruppe als die Gruppe auswählen, nach der gescannt werden soll.

Anzeigen von FDCC-Sicherheitsscanergebnissen

Die Ergebnisse des FDCC-Sicherheitsscans können entweder über das Extra "Sicherheits- und Patchmanagement" oder über das Fenster "Sicherheits- und Patchmanagement - Informationen" abgerufen werden.

Sollte eine Anfälligkeitsdefinition fehlschlagen, wird sie durch eine (1) in der Spalte "Erkannt" als erkannt angezeigt. Ist eine Anfälligkeitsdefinition erfolgreich, wird sie durch eine (0) in der Spalte "Erkannt" dargestellt.

HINWEIS: Darüber hinaus gibt es eine Anfälligkeitsdefinition, die alle Computer meldet, die das zum Bestehen des FDCC-Konfigurationsstandards geforderte Ergebnis nicht erreicht haben, d. h. nicht in Ordnung sind.

Hilfe zu Patch und Compliance

Das Extra-Fenster "Patch und Compliance" (**Extras > Sicherheit und Compliance > Patch und Compliance**) verwenden Sie, um Sicherheitsscans, Reparaturen und ähnliche Tasks auszuführen. Sie können Sicherheitsinhalte downloaden und verwalten, Sicherheits- und Compliancescans konfigurieren, Reparaturen konfigurieren, Einstellungen für die Anzeige und Interaktion mit dem Sicherheitsscanner anpassen und anwenden sowie umfassende sicherheitsbezogene Informationen zu gescannten Geräten anzeigen.

Der Hauptabschnitt zu "Patch und Compliance" auf Seite 578 bietet eine Einführung zu diesem Sicherheitsverwaltungstool. Dieser Abschnitt bietet einen Überblick und Informationen zum Abonnement für Sicherheitsinhalte und beschreibt Schritt für Schritt, wie Sie die verschiedenen Funktionen dieses Extras richtig einsetzen. Dort finden Sie auch eine Beschreibung der Schnittstelle und der Funktionen des Extras. Siehe "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584.

Dieser Abschnitt enthält die nachstehenden Hilfethemen, in denen die Dialogfelder von Patch und Compliance beschrieben werden. Von der Konsolenoberfläche aus können Sie diese Themen aufrufen, indem Sie auf die Schaltfläche **Hilfe** des jeweiligen Dialogfelds klicken.

- "Hilfe zum Fenster "Patch und Compliance"" auf Seite 653
- "Hilfe zum Download von Sicherheitsinhaltsupdates" auf Seite 654
- "Hilfe zu Definitionseigenschaften" auf Seite 659
- "Hilfe zu Erkennungsregeleigenschaften" auf Seite 662
- "Hilfe zu Patch- und Compliancetasks" auf Seite 671
- "Hilfe zu Patch und Compliance-Einstellungen" auf Seite 677
- "Hilfe zur Patch und Compliance-Symbolleiste" auf Seite 689

Hilfe zum Fenster "Patch und Compliance"

Informationen zum Dialogfeld "Spalten auswählen"

Dieses Dialogfeld verwenden Sie zum Konfigurieren von Datenspalten für Elementlisten im Extra-Fenster "Patch und Compliance". Sie entschieden, welche Datenspalten angezeigt werden. Auf diese Weise können Sie umfassende Listen mit heruntergeladenen Sicherheitsdefinitionen durchblättern und die für einen bestimmten Task oder eine bestimmte Situation benötigten Informationen schnell und bequem ausfindig machen können.

HINWEIS: Verwenden der Datenspalte CVE-Kennung
LANDesk Security Suite bietet Unterstützung für den Benennungsstandard nach CVE (Common Vulnerabilities and Exposures). Mit Patch und Compliance können Sie anhand des CVE-Namens nach Anfälligkeiten suchen und CVE-Informationen für heruntergeladene Anfälligkeitsdefinitionen anzeigen. Weitere Informationen zur CVE-Benennungskonvention, zur LANDesk Kompatibilität mit dem CVE-Standard und dazu, wie Sie mithilfe der CVE-Kennung individuelle Anfälligkeiten in Patch und Compliance finden können, finden Sie unter "Suchen nach Anfälligkeiten anhand ihres CVE-Namens" auf Seite 606.

Indem Sie Datenspalten hinzufügen und entfernen und sie in der Liste nach oben und unten verschieben (nach links und rechts in der Spaltenansicht), stellen Sie sicher, dass relevante Informationen im Vordergrund und in der Mitte angezeigt werden.

- **Verfügbare Spalten:** Listet die Datenspalten auf, die aktuell nicht im Fenster des Extras "Patch und Compliance" angezeigt werden, aber verfügbar sind, um zur Liste "Ausgewählte Spalten" hinzugefügt zu werden.
- **Ausgewählte Spalten:** Listet die Datenspalten auf, die aktuell im Fenster "Patch und Compliance" angezeigt werden. Die Datenspalten werden in einer Liste mit heruntergeladenen Sicherheitsdefinitionen von links nach rechts und in derselben Reihenfolge angezeigt, wie sie hier von

oben nach unten angezeigt werden.

- **Standardwerte:** Stellt die standardmäßig angezeigten Datenspalten wieder her.

Informationen zum Dialogfeld "Filter verwalten"

Dieses Dialogfeld verwenden Sie zur Verwaltung von Filtern, die Sie zum Anpassen des Sicherheitsinhalts, der in der Elementliste des Fensters "Patch und Compliance" angezeigt wird, einsetzen können. Mithilfe der Filter können Sie lange unübersichtliche Listen ordnen.

- **Neu:** Öffnet das Dialogfeld "Filtereigenschaften", in dem Sie die Einstellungen eines neuen Filters konfigurieren können.
- **Bearbeiten:** Öffnet das Dialogfeld "Filtereigenschaften", in dem Sie den ausgewählten Filter bearbeiten und speichern können.
- **Löschen:** Entfernt den ausgewählten Filter dauerhaft aus der Datenbank.
- **Filter verwenden:** Wendet den ausgewählten Filter auf die aktuelle Elementliste an. Der angewandte Filter wird beim Klicken auf andere Gruppen in der Strukturansicht übernommen.

Informationen zum Dialogfeld "Filtereigenschaften"

Mit diesem Dialogfeld erstellen oder bearbeiten Sie Filter für Sicherheitsinhaltslisten. Sie können nach Betriebssystem, Schweregrad des Sicherheitsrisikos oder beidem zusammen filtern.

- **Filtername:** Kennzeichnet den Filter mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Filter" angezeigt.
- **Betriebssysteme filtern:** Gibt die Betriebssysteme an, deren Definitionen Sie in den Elementlisten anzeigen möchten. Nur die mit den Betriebssystemen verknüpften Elemente, die von Ihnen ausgewählt wurden, werden angezeigt.
- **Schweregrade filtern:** Gibt die Schweregrade an, deren Definitionen Sie in den Elementlisten anzeigen möchten. Nur die Elemente, deren Schweregrad den von Ihnen ausgewählten Schweregraden entspricht, werden angezeigt.

Hilfe zum Download von Sicherheitsinhaltsupdates

Informationen zum Dialogfeld "Updates downloaden"

In diesem Dialogfeld konfigurieren Sie die Einstellungen für den Download von Updates für Sicherheitsinhalte, den Proxyserver, den Downloadspeicherort der Patchdatei, für Spyware-Autofix und für Antivirus-Updates und Sicherungen.

Führen Sie die folgenden Schritte aus, nachdem Sie angegeben haben, welche Art von Inhaltsupdate Sie downloaden möchten, und nachdem Sie die gewünschten Optionen auf den verschiedenen Seiten des Dialogfeld "Updates downloaden" festgelegt haben:

- Klicken Sie zum Ausführen eines sofortigen Downloads auf **Jetzt herunterladen**. Falls Sie auf **Übernehmen** klicken, werden die angegebenen Einstellungen gespeichert und beim nächsten Öffnen dieses Dialogfelds angezeigt. Falls Sie auf **Schließen** klicken, werden Sie gefragt, ob Sie die Einstellungen speichern möchten.

- Klicken Sie zum Planen eines Tasks für das Downloaden von Sicherheits- und Patchinhalten auf **Download planen**, um das Dialogfeld **Informationen zum geplanten Update** zu öffnen. Geben Sie einen Namen für den Task ein, überprüfen Sie die Informationen für den Task und klicken Sie dann auf **OK**, um den Task zu den geplanten Tasks hinzuzufügen.
- Sie können auf **Protokoll anzeigen** klicken, um die Protokolldatei zu öffnen.

Wenn Sie die Änderungen, die Sie auf einer der Seiten dieses Dialogfelds vorgenommen haben, speichern möchten, klicken Sie auf **Übernehmen**.

Das Dialogfeld **Updates downloaden** enthält die folgenden Seiten:

- "Informationen zur Seite "Updates"" auf Seite 655
- "Informationen zur Seite "Proxyeinstellungen"" auf Seite 657
- "Informationen zur Seite "Patchspeicherort"" auf Seite 658
- "Informationen zur Seite "LANDesk Antivirus"" auf Seite 658
- "Informationen zur Seite "Inhalt"" auf Seite 658
- "Informationen zur Seite "Import/Export"" auf Seite 658

WICHTIG: Besondere Überlegungen zum Download von Sicherheitsinhalt

Security Suite-Inhaltsabonnements

Eine Basisinstallation von LANDesk Management Suite ermöglicht es Ihnen, nach LANDesk Softwareupdates zu suchen und sie herunterzuladen sowie eigene benutzerdefinierte Definitionen zu erstellen und zu verwenden. Für alle anderen Sicherheitsinhalte, z. B. plattformspezifische Anfälligkeiten, Spyware etc., benötigen Sie ein LANDesk Security Suite-Inhaltsabonnement, das es Ihnen gestattet, die verknüpften Definitionen herunterzuladen.

Informationen zu den Security Suite-Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.

LANDesk Startseite

Taskspezifische Einstellungen und globale Einstellungen

Beachten Sie, dass nur die Definitionstyp-, Sprach- sowie Definitions- und Patch-Downloadeinstellungen gespeichert und mit einem spezifischen Task während dessen Erstellung verknüpft werden. Diese drei Einstellungen gelten als taskspezifisch.

Alle anderen Einstellungen auf den anderen Seiten des Dialogfeldes "Updates downloaden" sind global, d. h., sie gelten für alle nachfolgenden Downloadtasks für Sicherheitsinhalte. Die globalen Einstellungen umfassen: Patchdownload-Speicherort, Proxyserver, Spyware-Autofix, Sicherheitsalarme und Antivirus. Jedes Mal, wenn Sie eine globale Einstellung ändern, gilt diese Änderung für alle Sicherheitsinhalt-Downloadtasks von diesem Punkt an.

Informationen zur Seite "Updates"

- **Website der Updatequelle auswählen:** Gibt an, auf welchen LANDesk Inhaltsserver zugegriffen wird, um die neuesten Definitionen, Erkennungsregeln und entsprechenden Patches in Ihre Datenbank zu laden. Wählen Sie den Server aus, der Ihrem Standort am nächsten ist.

- **Definitionstypen:** Bestimmt, für welche Plattformen die Sicherheitsinhaltsdefinitionen aktualisiert werden. Es sind nur diejenigen Definitionstypen verfügbar, für die Sie ein Abonnement besitzen. Je mehr Definitionen Sie auswählen, umso länger dauert das Herunterladen.

  Nachdem Sie den Sicherheitsinhalt heruntergeladen haben, können Sie die Dropdownliste **Typ** im Hauptfenster des Tools "Patch und Compliance" zum Festlegen der Definitionstypen verwenden, die in einer Liste angezeigt werden sollen. Informationen über die Verwendung der Listenoptionen finden Sie unter "Dropdownliste "Typ"" auf Seite 587.

- **Sprachen:** Identifiziert die Sprachversionen der ausgewählten Definitionstypen, die aktualisiert werden.

  Einige Anfälligkeiten und Definitionstypen sowie damit verknüpfte Patches sind sprachneutral oder unabhängig, d. h., sie sind mit jeder Sprachversion des Betriebssystems oder Anwendung kompatibel, die von dieser Definition adressiert wird. Sie benötigen demnach keinen eindeutigen sprachspezifischen Patch, um diese Anfälligkeiten zu reparieren, da das Patch alle unterstützten Sprachen abdeckt. Linux-und UNIX-Plattformen verwenden beispielsweise nur sprachneutrale Definitionen und Patches. Microsoft Windows und Apple Macintosh verwenden jedoch fast ausschließlich sprachspezifische Anfälligkeitsdefinitionen und Patches.

  Beim Downloaden des Inhalts für eine bestimmte Plattform (mit dem entsprechenden Sicherheitsinhaltsabonnement) werden pro Standardeinstellung alle sprachneutralen Anfälligkeitsdefinitionen der ausgewählten Plattform automatisch aktualisiert. Wenn Sie einen Windows- oder Mac-Inhaltstyp ausgewählt haben, müssen Sie zudem die Sprachen auswählen, deren Definitionen Sie aktualisieren möchten. Wenn Sie die Sun Solaris- oder eine Linux-Plattform ausgewählt haben, müssen Sie keine Sprache auswählen, da ihr Inhalt sprachneutral ist und automatisch aktualisiert wird.

- **Die oben ausgewählten Patches für Definitionen downloaden:** Ausführbare Patchdateien werden automatisch in den angegebenen Speicherort für Downloads heruntergeladen (siehe Seite "Patchspeicherort"). Dabei wird eine der folgenden Downloadoptionen berücksichtigt:
  - **Nur für erkannte Definitionen:** Downloadet nur die Patches, die mit Anfälligkeiten, Sicherheitsbedrohungen oder LANDesk Updates verknüpft sind, die vom letzten Sicherheitsscan erkannt wurden (d. h. die Definitionen, die sich derzeit in der Gruppe "Erkannt" befinden).
  - **Für alle gedownloadeten Definitionen:** Downloadet ALLE Patches, die mit Anfälligkeiten, Sicherheitsbedrohungen und LANDesk Softwareupdates verknüpft sind, die sich derzeit in der Gruppe "Scannen" befinden.
- **Automatische Patchbereitstellung mit Process Manager aktivieren:** Gestattet Ihnen die Konfiguration der LANDesk Process Manager-Datenbank, die Sie zur Verwendung der integrierten, automatischen Patchbereitstellungsfunktion benötigen.
- **LANDesk Process Manager** Klicken Sie auf die Schaltfläche, um das Dialogfeld "Automatische Patchbereitstellung" zu öffnen, das die integrierte Funktion zwischen LANDesk Process Manager und dem Tool "Patch und Compliance" beschreibt, mit dem Sie einen Workflow erstellen können, um die Patchbereitstellung auf Zielgeräten zu automatisieren. Sie können auch eine schrittweise Anleitung aufrufen, die Sie durch dieses Verfahren führt. LANDesk Process Manager umfasst Hilfethemen mit ausführlichen Informationen über seine Funktionen und ihre Verwendung, auf die Sie jederzeit zugreifen können.

- **Neue Definitionen der Gruppe "Nicht zugewiesen" zuordnen (wenn nicht durch Definitionsgruppeneinstellungen außer Kraft gesetzt):** Fügt neue Definitionen und damit verknüpfte Erkennungsregeln in die Gruppe "Nicht zugewiesen", anstatt in die Standardgruppe "Scannen" ein. Wählen Sie diese Option, wenn Sie die Möglichkeit einrichten möchten, Inhalte manuell in und aus der Gruppe "Scannen" zu verschieben, um den Sicherheitsscan anzupassen.

  HINWEIS: Definitionen, die in einem Abhängigkeitsverhältnis zu anderen Definitionen stehen, die bereits in einer anderen Gruppe vorhanden sind, wie beispielsweise die Gruppe "Scannen" oder die Gruppe "Nicht scannen", werden bei Auswahl dieser Option automatisch in diese Gruppe gestellt. Anders ausgedrückt bedeutet dies, dass das Abhängigkeitsverhältnis diese Option außer Kraft setzt, so dass die zuletzt heruntergeladene (neue Definition) in derselben Gruppe steht, wie die Definition, zu der das Abhängigkeitsverhältnis besteht.

  HINWEIS: Definitionen, die zum Einfügen in die Gruppe "Alarm" ausgewählt wurden (im Dialogfeld **Alarme konfigurieren**), werden automatisch auch in die Gruppe "Scannen" eingefügt, selbst wenn diese Option ausgewählt ist, so dass die entsprechende Alarmierung stattfindet.

  HINWEIS: Der Standardspeicherort für den Download ist beim Anwendungstyp "Blockiert" ein anderer. Für blockierte Anwendungen werden Definitionen standardmäßig in die Gruppe "Nicht zugewiesen" heruntergeladen, nicht in die Gruppe "Scannen". Sie brauchen diese Option nicht auszuwählen, wenn Sie nur Definitionen für blockierte Anwendungen downloaden.

- **Definitionsgruppeneinstellungen:** Öffnet das Dialogfeld "Definitionsgruppeneinstellungen". Hier können Sie Definitionsgruppen erstellen, verwalten und auswählen. Sie können Definitionsgruppeneinstellungen dazu verwenden, das Downloaden, den Scanzustand und den Downloadspeicherort der Sicherheitsdefinitionen (Inhalt), die dem angegebenen Typ und Schweregradkriterien entsprechen, automatisch einzustellen.

Informationen zur Seite "Proxyeinstellungen"

Wenn Ihr Netzwerk einen Proxyserver für externe Übertragungen (z. B. Internetzugriff) nutzt, aktivieren und konfigurieren Sie auf dieser Seite die Einstellungen für den Proxyserver. Für die Aktualisierung der Anfälligkeitsinformationen und den Download der Patchdateien von den entsprechenden Webdiensten ist ein Internetzugang erforderlich.

- **Proxyserver verwenden:** Aktiviert die Proxyserver-Option (die Option ist standardmäßig deaktiviert). Wenn Sie einen Proxyserver aktivieren, müssen Sie die Adresse und den Port in die unten stehenden Felder eingeben.
- **Server:**
  - **Adresse:** Gibt die IP-Adresse Ihres Proxyservers an.
  - **Port:** Gibt die Portnummer Ihres Proxyservers an.
- **HTTP-basierter Proxy:** Aktiviert den Proxyserver, wenn es sich um einen HTTP-basierten Proxy handelt (wie z. B. Squid), damit der Server Verbindungen mit FTP-Sites herstellen und von diesen Sites Patches downloaden kann. (Auf bestimmten FTP-Sites bereitgestellte Patches können erst dann über einen HTTP-basierten Proxy heruntergeladen werden, wenn Sie zuvor diese Option aktivieren).
- **Erfordert Anmeldung:** Ermöglicht die Eingabe eines Benutzernamens und eines Kennworts, wenn der Proxyserver Anmeldeinformationen verlangt und kein transparenter Proxyserver ist.
  - **Benutzername:** Geben Sie einen gültigen Benutzernamen und Anmeldeinformationen für die

Authentifizierung gegenüber dem Proxyserver ein.

- **Kennwort:** Geben Sie das Kennwort des Benutzers ein.

Informationen zur Seite "Patchspeicherort"

Verwenden Sie diese Seite, um anzugeben, in welchen Speicherort Patches heruntergeladen werden.

- **UNC-Pfad, in dem Patches gespeichert werden:** Gibt an, wohin die Patchdateien heruntergeladen werden. Der Standardspeicherort ist der Ordner \LDLogon\Patch des Coreservers. Sie können einen anderen UNC-Pfad für den Download von Patches eingeben. Dabei müssen Sie jedoch sicherstellen, dass ein Zugriff auf den Speicherort erfolgen kann, indem Sie gültige Anmeldeinformationen für die Authentifizierung in die unten stehenden Felder eingeben.
- **Anmeldeinformationen zum Speichern von Patches:** Enthält einen gültigen Benutzernamen und ein Kennwort für den Zugriff auf einen anderen Speicherort als den Coreserver. Wenn Sie Patches in den Standardspeicherort auf dem Coreserver downloaden, sind die Felder "Benutzername" und "Kennwort" nicht aktivierbar.
- **Web-URL oder UNC-Pfad für den Clientzugriff auf Patches:** Gibt eine Webadresse an, über die Geräte auf heruntergeladene Patches zwecks Bereitstellung zugreifen können. Der Standardspeicherort ist der Ordner \LDLogon\Patch des Coreservers. Dieser Speicherort entspricht in der Regel dem oben angegebenen UNC-Pfad.
- **Einstellungen testen:** Führt eine Konnektivitätsprüfung zur angegebenen URL durch.
- **Auf Standard zurücksetzen:** Setzt den UNC-Pfad und die URL-Adresse auf den Standardspeicherort zurück, der dem Ordner \LDLogon\Patch des Coreservers entspricht.

Informationen zur Seite "LANDesk Antivirus"

Diese Seite verwenden Sie um Downloadoptionen für LANDesk Antivirus Virendefinitionsdateien zu konfigurieren. Denken Sie daran, dass diese Seite sich nur auf von LANDesk Antivirus verwendete Virendefinitionsdateien bezieht, nicht auf den von Antivirus-Scannern erkannten Inhalt (Antivirus-Updates), der in der Definitionsliste auf der Seite **Updates** bereitgestellt wird.

Ausführliche Informationen finden Sie unter "Informationen zur Seite "LANDesk Antivirus" im Dialogfeld "Updates downloaden"" auf Seite 776.

Informationen zur Seite "Inhalt"

Sie verwenden diese Seite für Folgendes:

- **Verifizieren von Definitionssignaturen/-Hashes vor dem Download:**

Informationen zur Seite "Import/Export"

Diese Seite verwenden Sie zur Konfiguration des Imports oder Exports von Antivirus-Einstellungen.

- **Einstellungen aus Datei importieren:**
- **Einstellungen in Datei exportieren:**
- **Einstellungen auf anderen Core kopieren:**

Hilfe zu Definitionseigenschaften

Informationen zum Dialogfeld "Definitionseigenschaften"

Dieses Dialogfeld verwenden Sie, um Eigenschaften von heruntergeladenen Inhaltsdefinitionstypen, einschließlich Anfälligkeiten, Spyware, Sicherheitsbedrohungen, Softwareaktualisierungen etc., anzuzeigen.

Sie können mit dieser Seite auch eigene benutzerdefinierte Definitionen erstellen.

Diese Informationen sind bei heruntergeladenen Definitionen schreibgeschützt. Bei benutzerdefinierten Definitionen sind die Felder in diesem Dialogfeld editierbar. Sie können mit den verfügbaren Felder in diesem Dialogfeld und im Dialogfeld mit den Erkennungsregeleigenschaften Kennungs-, Attribut- und Erkennungsregeldetails für eine benutzerdefinierte Definition eingeben.

Verwenden Sie die nach links und rechts zeigenden Pfeilschaltflächen (<, >), um Informationen zu den Eigenschaften der vorherigen oder nächsten Definition anzuzeigen; die Definitionen werden in der Reihenfolge angezeigt, in der sie derzeit im Hauptfenster aufgelistet sind.

Das Dialogfeld "Definitionseigenschaften" umfasst die folgenden Seiten:

- "Informationen zur Definition: Seite "Allgemein"" auf Seite 659
- "Informationen zur Definition: Seite "Beschreibung"" auf Seite 660
- "Informationen zur Definition: Seite "Abhängigkeiten"" auf Seite 660
- "Informationen zur Definition: Seite "Benutzerdefinierte Variablen"" auf Seite 660

Informationen zur Definition: Seite "Allgemein"

- **Kennung:** Identifiziert die ausgewählte Definition mit einem eindeutigen, vom Anbieter definierten alphanumerischen Code (oder benutzerdefinierter Code bei benutzerdefinierten Definitionen).
- **Typ:** Weist das ausgewählte Element als eine Anfälligkeit, Sicherheitsbedrohung, benutzerdefinierte Definition etc. aus.
- **Veröffentlichungsdatum:** Gibt das Datum an, an dem die Definition vom Anbieter veröffentlicht (oder von einem Benutzer erstellt) wurde.
- **Titel:** Beschreibt Art oder Ziel der ausgewählten Definition in einem kurzen Text.
- **Schweregrad:** Gibt den Schweregrad der Definition an. Bei heruntergeladenem Inhalt wird der Schweregrad vom Anbieter zugewiesen. Bei einer benutzerdefinierten Definition wird der Schweregrad von demjenigen Benutzer zugewiesen, der die Definition erstellt hat. Mögliche Schweregrade sind: "Service Pack", "Kritisch", "Hoch", "Mittel", "Niedrig", "Nicht anwendbar" und "Unbekannt". Verwenden Sie diese Informationen, um das mit der Definition verbundene Risiko zu bewerten und um einzuschätzen, wie wichtig Scan- und Reparaturvorgänge für Ihr Netzwerk sind.
- **Status:** Gibt den Status der Definition im Fenster "Patch und Compliance" an. Es gibt drei Statusindikatoren: "Scannen" bedeutet, dass das ausgewählte Element für den nächsten Sicherheitsscan aktiviert wurde, "Nicht scannen", dass es nicht in den Scan einbezogen wird, und "Nicht zugewiesen", dass es sich in einem temporären Wartebereich befindet und nicht gescannt wird. Weitere Informationen zu den drei Statusmöglichkeiten bzw. Gruppen finden Sie unter "Grundlegendes zum Inhalt und zur Verwendung des Extra-Fensters "Patch und Compliance"" auf Seite 584.
- **Sprache:** Gibt die Sprache der von der Definition identifizierten Plattform an. Bei benutzerdefinierten Definitionen ist INTL der Standardwert. Das heißt, die Definition ist sprachunabhängig und lässt sich nicht bearbeiten.
- **Kategorie:** Gibt eine spezifischere Kategorie innerhalb eines Sicherheitsinhaltstyps an (siehe oben).

- **Erkennungsregeln:** Listet die mit der ausgewählten Definition verknüpften Erkennungsregeln auf. Beachten Sie, dass der Eintrag **Gedownloadet** angibt, ob die Patchdatei in das lokale Repository heruntergeladen wurde, und der Eintrag **Unbeaufsichtigte Installation**, ob das Patch ohne Benutzerbeteiligung installiert wird.

Sie können mit der rechten Maustaste auf eine Erkennungsregel klicken, um das zugehörige Patch (oder Patches) herunterzuladen, die Erkennungsregel für Sicherheitsscans zu deaktivieren/aktivieren, die zugehörigen Patches zu deinstallieren oder ihre Eigenschaften anzuzeigen. Sie können auch auf eine Erkennungsregel doppelklicken, um ihre Eigenschaften anzuzeigen.

Klicken Sie beim Arbeiten mit einer benutzerdefinierten Definition auf **Hinzufügen**, um eine neue Erkennungsregel zu erstellen. Klicken Sie auf **Bearbeiten**, um die ausgewählte Regel zu ändern, oder auf **Löschen**, um sie zu löschen.

Informationen zur Definition: Seite "Beschreibung"

- **Beschreibung:** Stellt zusätzliche Details zur ausgewählten Definition bereit. Diese Informationen finden Sie in den Entwicklungs- und Testhinweisen des Anbieters (oder sie werden von dem Benutzer zur Verfügung gestellt, der die benutzerdefinierte Definition erstellt hat).
- **Weitere Informationen:** Enthält einen HTTP-Link zu einer anbieterspezifischen (oder benutzerdefinierten) Webseite, für gewöhnlich eine Support-Site, die weitere Informationen zur ausgewählten Definition enthält.
- **Weitere Informationen zur CVE-Kennung:** (Gilt nur für Anfälligkeiten) Stellt die CVE-Kennung (Name) für die ausgewählte Anfälligkeit bereit sowie einen Link zur CVE-Website für die betreffende CVE-Kennung. Weitere Informationen finden Sie unter "Suchen nach Anfälligkeiten anhand ihres CVE-Namens" auf Seite 606.

Informationen zur Definition: Seite "Abhängigkeiten"

Diese Seite wird nur angezeigt, wenn die ausgewählte Definition über eine zugeordnete vorgeschriebene Definition verfügt, oder wenn die Ausführung einer anderen Definition von der ausgewählten Definition abhängt. Sie können diese Seite verwenden, um vor dem Scannen von Geräten sicherzustellen, dass Ihr Sicherheitsscantask alle zur ordnungsgemäßen Ausführung erforderlichen Definitionen enthält.

Eine Abhängigkeitsbeziehung kann nur für die folgenden Sicherheitsdefinitionstypen bestehen:

- **Voraussetzungen:** Listet Definitionen auf, die ausgeführt werden müssen, BEVOR die ausgewählte Definition auf Geräten geprüft werden kann. Wenn eine der Definitionen in dieser Liste nicht in den Scantask eingeschlossen wird, wird die ausgewählte Definition vom Sicherheitsscanner nicht erkannt.
- **Abhängigkeiten:** Listet Definitionen auf, die erst NACH der Ausführung der ausgewählten Definition von Sicherheitsscanner erkannt werden. Beachten Sie, dass die ausgewählte Definition auch dann gescannt wird, wenn diese Definitionen nicht im Sicherheitsscan-Task eingeschlossen sind. Wenn der Scantask eine Definition in dieser Liste jedoch erfolgreich erkennen soll, muss die ausgewählte Definition zuerst ausgeführt werden.

Informationen zur Definition: Seite "Benutzerdefinierte Variablen"

Diese Seite wird NUR angezeigt, wenn die ausgewählte Sicherheitsdefinition Einstellungen oder Werte enthält, die geändert werden können. Einige Definitionen für Sicherheitsbedrohungen der Systemkonfiguration verfügen beispielsweise über Einstellungen, die Sie ändern können, bevor Sie sie in einem Sicherheitsscan einschließen. Normalerweise verfügen Virenschutzdefinitionen auch über Einstellungen für benutzerdefinierte Variablen.

Mit benutzerdefinierten Variablen können Sie das Scannen auf Sicherheitsbedrohungen optimieren, indem Sie die Werte einer oder mehrerer Einstellungen so ändern, dass der Scanner nach von Ihnen definierten Bedingungen sucht und das Gerät nur dann als anfällig erkennt, wenn diese spezielle Bedingung erfüllt ist (d. h. der von Ihnen angegebene Wert vorgefunden wird).

WICHTIG: Das Recht "Benutzerdefinierte Variablen bearbeiten" ist erforderlich
Um Einstellungen benutzerdefinierter Variablen bearbeiten zu können, muss der LANDesk Benutzer über das rollenbasierte Administrationsrecht "Benutzerdefinierte Variablen bearbeiten" verfügen. Rechte werden mit dem Extra **Benutzer** konfiguriert.

Jede Sicherheitsdefinition, die über benutzerdefinierte Variablen verfügt, besitzt einen eindeutigen Satz spezifischer änderbarer Werte. In jedem Fall werden auf der Seite **Benutzerdefinierte Variablen** jedoch die folgenden Informationen zu sehen sein:

- **Name:** Identifiziert die benutzerdefinierte Variable. Der Name kann nicht geändert werden.
- **Wert:** Gibt den aktuellen Wert der benutzerdefinierten Variable an. Sie können auf dieses Feld doppelklicken, um den Wert zu ändern, es sei denn, die Variable ist schreibgeschützt.
- **Variable hinzufügen:** Öffnet ein Dialogfeld, in dem Sie Ihre eigene benutzerdefinierte Variable erstellen können. (HINWEIS: Bevor Sie eine benutzerdefinierte Variable für eine benutzerdefinierte Anfälligkeitsdefinition erstellen können, muss die Definition mindestens eine Erkennungsregel enthalten.)
- **Variable bearbeiten:** Damit können Sie die ausgewählte benutzerdefinierte Variable bearbeiten.
- **Variable entfernen:** Löscht die ausgewählte benutzerdefinierte Variable.
- **Beschreibung:** Stellt zusätzliche nützliche Informationen zur benutzerdefinierten Variable bereit, die vom Autor der Definition stammen.
- **Standardwert:** Stellt den Standardwert bereit, falls Sie diesen geändert haben und den ursprünglichen Wert wiederherstellen möchten.

Um eine benutzerdefinierte Variable zu ändern, doppelklicken Sie auf das Feld **Wert** und wählen entweder einen Wert aus, wenn es eine Dropdownliste gibt, oder bearbeiten den Wert ansonsten manuell, und klicken dann auf **Übernehmen**. Beachten Sie, dass einige Variablen schreibgeschützt sind und nicht bearbeitet werden können (dies wird normalerweise in der Beschreibung vermerkt).

Informationen zur den Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen werden in der Inventaransicht des Geräts angezeigt.

HINWEIS: Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen
In manchen Situationen sollten Sie benutzerdefinierte Variableneinstellungen ggf. ignorieren oder – anders ausgedrückt – eine Ausnahme von der Regel erstellen. Hierfür steht in eine Funktion mit dem Namen "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen" zur Verfügung. Mithilfe der Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen können Sie entscheiden, welche benutzerdefinierten Variablen beim Scannen von Geräten ignoriert werden, damit sie nicht als anfällig erkannt und repariert werden, selbst wenn sie eigentlich die Bedingungen der Erkennungsregeln einer Definition erfüllen. Sie können beliebig viele Einstellungen zur Außerkraftsetzung benutzerdefinierter Variablen erstellen und diese dann mit einem Task vom Typ **Einstellungen ändern** auf Geräte anwenden. Weitere Informationen hierzu finden Sie unter "Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen"" auf Seite 685.

Informationen zum Dialogfeld "Benutzerdefinierte Variable hinzufügen/bearbeiten"

Dieses Dialogfeld verwenden Sie zur Erstellung und Bearbeitung Ihrer eigenen benutzerdefinierten Variablen für Ihre benutzerdefinierten Anfälligkeitsdefinitionen. Mit benutzerdefinierten Variablen können Sie das Scannen auf Sicherheitsbedrohungen optimieren, indem Sie die Werte einer oder mehrerer Einstellungen so ändern, dass der Scanner nach von Ihnen definierten Bedingungen sucht und das Gerät nur dann als anfällig erkennt, wenn diese spezielle Bedingung erfüllt ist (d. h. der von Ihnen angegebene Wert vorgefunden wird).

WICHTIG: Bevor Sie eine benutzerdefinierte Variable für eine benutzerdefinierte Anfälligkeitsdefinition erstellen können, muss die Definition mindestens eine Erkennungsregel enthalten.

Dieses Dialogfeld enthält folgende Optionen:

- **Name:** Identifiziert die benutzerdefinierte Variable.
- **Beschreibung:** Zur Angabe zusätzlichen nützlicher Informationen über die benutzerdefinierte Variable.
- **Typ:** Identifiziert den Ressourcentyp, der für die Definition der benutzerdefinierten Variablen verwendet wurde (mögliche Typen sind "Zeichenfolge", "Verschlüsselte Zeichenfolge", "Mehrwertige Zeichenfolge", "Ganzzahl", "Aufzählung" und "Boolesch").
- **Mögliche Werte:** Hier geben Sie alle möglichen Werte ein, die für die von Ihnen erstellte benutzerdefinierte Variable (basierend auf dem oben angegebenen Typ) als gültige Werte gelten sollen.
- **Standardwert:** Hier geben Sie den Standardwert der benutzerdefinierten Variable an.

Hilfe zu Erkennungsregeleigenschaften

Informationen zum Dialogfeld "Erkennungsregeleigenschaften"

Dieses Dialogfeld verwenden Sie zum Anzeigen der Eigenschaften von heruntergeladenem Sicherheitsinhalt oder zum Erstellen und Bearbeiten benutzerdefinierter Erkennungsregeln.

Diese Informationen sind bei Erkennungsregeln, die zu heruntergeladenen Definitionen gehören, schreibgeschützt. Bei benutzerdefinierten Definitionen sind die Felder auf den Seiten dieses Dialogfelds editierbar. Mit den Einstellungen für Erkennungsregeln und den Optionen auf den jeweiligen Seiten können Sie benutzerdefinierte Erkennungsregeln konfigurieren. Wenn die benutzerdefinierte Erkennungsregel Reparaturen zulässt, können Sie zudem Sonderbefehle hinzufügen, die während des Reparaturvorgangs (Patchinstallation oder -deinstallation) ausgeführt werden.

Mit den linken und rechten Pfeilschaltflächen (<, >) können Sie Eigenschaftsdaten zur vorherigen bzw. nächsten Erkennungsregel anzeigen. Die Reihenfolge beim Anzeigen entspricht der aktuellen Reihenfolge der Erkennungsregeln im Hauptfenster.

Das Dialogfeld "Erkennungsregeleigenschaften" enthält folgende Seiten:

- "Informationen zur Seite "Erkennungsregel: Allgemeine Informationen"" auf Seite 663
- "Informationen zur Seite "Erkennungslogik: Betroffene Plattformen"" auf Seite 663
- "Informationen zur Seite "Erkennungslogik: Betroffene Produkte"" auf Seite 663
- "Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Dateien"" auf Seite 664
- "Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Registrierungseinstellungen"" auf Seite 665

- "Informationen zur Seite "Erkennungslogik: Benutzerdefiniertes Skript"" auf Seite 665
- "Informationen zur Seite "Patchinformationen"" auf Seite 666
- "Informationen zur Seite "Erkennung des Patches: Zur Erkennung installierter Patches verwendete Dateien"." auf Seite 667
- "Informationen zur Seite "Erkennung des Patches: Zur Erkennung installierter Patches verwendete Registrierungseinstellungen"." auf Seite 668
- "Informationen zur Seite "Patchinstallationsbefehle"" auf Seite 668
- "Informationen zur Seite "Patchdeinstallationsbefehle"" auf Seite 670

Informationen zur Seite "Erkennungsregel: Allgemeine Informationen"

- **Name:** Zeigt den Namen der Erkennungsregel an.
- **Status:** Gibt an, ob die Erkennungsregel auf "scannen" oder "nicht scannen" gesetzt wurde. Diese beiden Zustände entsprechen den Gruppen "Scannen" und "Nicht scannen" (unter "Erkennungsregeln" im Fenster "Patch und Compliance").
- **Kennung:** Zeigt die Kennung der Definition an, die mit dieser Regel verknüpft ist.
- **Titel:** Zeigt den Titel der zu dieser Regel gehörenden Definition an.
- **Beschreibung:** Zeigt die Beschreibung der zu dieser Regel gehörenden Definition an.
- **Kommentare:** Zeigt zusätzliche Informationen des Anbieters, falls verfügbar. Wenn Sie eine benutzerdefinierte Definition erstellen oder bearbeiten, können Sie eigene Kommentare einfügen.

Erkennungslogik-Seiten

Die nachstehenden Seiten beschreiben die Erkennungslogik, mit der die ausgewählte Erkennungsregel entscheidet, ob die Anfälligkeitsdefinition (oder ein anderer Definitionstyp) auf einem gescannten Gerät existiert.

Informationen zur Seite "Erkennungslogik: Betroffene Plattformen"

Weist die Betriebssysteme aus, auf denen der Anfälligkeitsscanner ausgeführt wird, um nach der mit dieser Regel verknüpften Anfälligkeit zu suchen. Das heißt, nur Geräte, die mit den ausgewählten Plattformen übereinstimmen, werden versuchen, diese Regel abzuarbeiten. Es MUSS mindestens eine Plattform ausgewählt werden. Wenn ein Zielgerät ein anderes Betriebssystem ausführt, wird der Sicherheitsscan abgebrochen.

Informationen zur Seite "Erkennungslogik: Betroffene Produkte"

- **Produkte:** Listet die Produkte auf, die Sie mit der Erkennungsregel ausfindig machen möchten, um zu bestimmen, ob die verknüpfte Definition auf gescannten Geräten existiert. Wählen Sie ein Produkt in der Liste aus, um den Namen, Anbieter und die Versionsinformationen des Produkts anzuzeigen. Sie müssen nicht unbedingt ein Produkt mit einer Erkennungsregel verknüpfen. Verknüpfte Produkte fungieren als Filter während des Sicherheitsscans. Wenn keine der angegebenen verknüpften Produkte auf dem Gerät gefunden werden, wird der Sicherheitsscan abgebrochen. Werden jedoch keine Produkte angegeben, setzt der Scanner die Dateiprüfung fort.

Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie durch Klicken auf **Konfigurieren** ein neues Dialogfeld öffnen, mit dem Sie Produkte zur Liste hinzufügen oder daraus entfernen können. Welche Produkte als verfügbar in der Liste angezeigt werden, hängt davon ab, welchen Sicherheitsinhalt Sie mithilfe des LANDesk Security Suite Webdienstes aktualisiert haben.

- **Name:** Der Name des ausgewählten Produkts.
- **Anbieter:** Der Namen des Anbieters.
- **Version:** Die Versionsnummer des ausgewählten Produkts.

Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Dateien"

- **Dateien:** Listet die Dateibedingungen (Präsenz, Version, Datum, Größe etc.) auf, mit denen ermittelt wird, ob die verknüpfte Definition auf gescannten Geräten existiert. Wählen Sie eine Datei in der Liste aus, um deren Überprüfungsmethode und erwarteten Parameter anzuzeigen. Wenn alle Dateibedingungen erfüllt werden, ist das Gerät nicht betroffen. Oder anders ausgedrückt, wenn eine dieser Dateibedingungen NICHT erfüllt wird, gilt die Anfälligkeit als auf diesem Gerät präsent. Wenn es keine Dateibedingungen in der Liste gibt, setzt der Scan die Registrierungsprüfung fort.
  Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie auf **Hinzufügen** klicken, um Felder editierbar zu machen. Auf diese Weise können Sie eine neue Dateibedingung und erwartete Werte/Parameter konfigurieren. Eine Regel kann eine oder mehrere Dateibedingungen einschließen, je nachdem, wie komplex Sie die Regel gestalten möchten. Zum Speichern einer Dateibedingung klicken Sie auf **Aktualisieren**. Zum Löschen einer Dateibedingung aus der Liste wählen Sie die betreffende Bedingung aus und klicken auf **Entfernen**.
- **Überprüfen mit:** Zeigt an, welche Methode zur Überprüfung verwendet werden soll, wenn die angegebene Dateibedingung auf den gescannten Geräten vorgefunden wird. Beispiel: Eine Erkennungsregel kann auf "Dateiexistenz", "Version", "Datum", "Größe" etc. prüfen. Die erwarteten Parameter, die unterhalb der Prüfmethode angezeigt werden, werden durch die Methode selbst bestimmt (siehe nachstehende Liste).

  Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie die Prüfmethode auswählen, indem Sie auf die Dropdownliste **Überprüfen unter Verwendung von** klicken. Wie oben angegeben variieren die Parameterfelder je nach Prüfmethode. Eine Beschreibung der Parameter finden Sie in der nachstehenden Liste.

  Beachten Sie, dass die Option **Rekursiv nach Datei suchen** auf alle Dateiverifizierungsmethoden zutrifft (mit Ausnahme der MSI-Methoden) und veranlasst, dass der Scan nach Dateien in dem angegebenen Pfadspeicherort und allen bestehenden untergeordneten Ordnern sucht.

- **Nur Dateiexistenz:** Prüft, indem nach der angegebenen Datei gesucht wird. Zulässige Parameter: Pfad (Speicherort der Datei auf der Festplatte) einschließlich Dateiname) und Voraussetzung (muss existieren oder muss nicht existieren).
- **Dateiversion:** Prüft, indem nach der angegebenen Datei und ihrer Versionsnummer gesucht wird. Zulässige Parameter: Pfad, Mindestversion und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).

Beachten Sie, dass Sie für die Parameter "Dateiversion", "Datum" und "Größe", nachdem Sie den Dateipfad und -namen angegebenen haben, auf die Schaltfläche **Daten sammeln** klicken können, um die entsprechenden Wertefelder automatisch mit Daten zu füllen.

- **Dateidatum:** Prüft, indem nach der angegebenen Datei und dem Datum gesucht wird. Zulässige Parameter: Pfad, Mindestdatum und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).
- **Dateigröße und/oder Prüfsumme:** Prüft, indem nach der angegebenen Datei und deren Größe und Prüfsummenwert gesucht wird. Zulässige Parameter: Pfad, Prüfsumme, Dateigröße und Voraussetzung (muss existieren, muss nicht existieren, kann existieren).
- **MSI Produkt-Kennung installiert:** Führt einen Scan durch, um sicherzustellen, dass das MSI-Produkt installiert ist (ein von Microsoft Installer installiertes Produkt). Zulässige Parameter: Guid (die globale eindeutige Produktkennung).

- **MSI Produkt-Kennung NICHT installiert:** Führt einen Scan durch, um sicherzustellen, dass das angegebene MSI-Produkt nicht installiert ist. Zulässige Parameter: Guid.

Informationen zur Seite "Erkennungslogik: Zur Erkennung verwendete Registrierungseinstellungen"

- **Registrierung:** Listet die Registrierungsschlüssel-Bedingungen auf, mit denen entschieden wird, ob die verknüpfte Anfälligkeit (oder ein anderer Typ) auf einem gescannten Gerät existiert. Wählen Sie einen Registrierungsschlüssel in der Liste aus, um dessen erwartete Parameter anzuzeigen. Wird eine dieser Bedingungen NICHT erfüllt, so gilt die Anfälligkeit als auf diesem Gerät präsent.

WICHTIG: Wenn keine Registrierungsbedingungen in der Liste aufgeführt werden UND keine Dateibedingungen auf der Seite "Dateien" angegeben waren, misslingt der Scan. Mit anderen Worten – eine Erkennungsregel muss mindestens eine Datei- oder Registrierungsbedingung enthalten.

Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, können Sie auf **Hinzufügen** klicken, um Felder editierbar zu machen. Auf diese Weise können Sie eine neue Bedingung für den Registrierungsschlüssel und erwartete Parameter konfigurieren. Eine Regel kann eine oder mehrere Registrierungsbedingungen umfassen. Zum Speichern einer Registrierungsbedingung klicken Sie auf **Aktualisieren**. Um eine Registrierungsbedingung aus der Liste zu löschen, wählen Sie die betreffende Bedingung aus und klicken auf **Entfernen**.

- **Schüssel:** Benennt den erwarteten Ordner und Pfad des Registrierungsschlüssels.
- **Name:** Benennt den erwarteten Namen des Schlüssels.
- **Wert:** Benennt den erwarteten Wert des Schlüssels.
- **Anforderung:** Zeigt an, ob der Registrierungsschlüssel auf Zielgeräten existieren muss oder nicht.

Informationen zur Seite "Erkennungslogik: Benutzerdefiniertes Skript"

Verwenden Sie diese Seite, wenn Sie ein benutzerdefiniertes VB-Skript schreiben möchten, das nach beliebigen anderen Bedingungen auf gescannten Geräten sucht. Die Runtime-Eigenschaften des Sicherheitsscanners, auf die zum Abrufen von Ergebnisberichten mit einem benutzerdefinierten Skript zugegriffen werden kann, lauten: "Erkannt", "Grund", "Erwartet" und "Gefunden".

Klicken Sie auf die Schaltfläche **Editor verwenden**, um das mit diesem Dateityp assoziierte Standard-Skriptbearbeitungstool zu öffnen. Beim Schließen des Tools werden Sie aufgefordert, Ihre Änderungen auf der Seite "Benutzerdefiniertes Skript" zu speichern. Wenn Sie ein anderes Tool verwenden möchten, müssen Sie die Dateitypverknüpfung ändern.

Informationen zu den Produkteigenschaften benutzerdefinierter Anfälligkeiten: Allgemeine Informationen"

Verwenden Sie diese Dialogfelder zum Erstellen einer benutzerdefinierten Anfälligkeitsdefinition, die ein angepasstes Produkt enthält.

Sie können einen Namen, Hersteller und eine Versionsnummer eingeben und dann die Erkennungslogik definieren, die die Bedingungen für das Bestehen einer Anfälligkeit bestimmt.

Diese Dialogfelder entsprechen den Eigenschaftsdialogfelder für heruntergeladene, veröffentlichte Anfälligkeitsdefinitionen. Sehen Sie sich bitte die entsprechenden Abschnitte oben an.

Diese Seite enthält folgende Optionen:

- **Betroffene Produkte:** Führt die von dieser benutzerdefinierten Anfälligkeitsdefinition betroffenen Produkte auf.

- **Verfügbare Produkte:** Führt alle heruntergeladenen Produkte auf.
- **Verfügbare Produkte nach betroffenen Plattformen filtern:** Beschränkt die Liste der verfügbaren Produkte auf solche, die mit Ihren in der Erkennungslogik ausgewählten Plattformen verknüpft sind: Seite "Betroffene Plattformen"
- **Hinzufügen:** Öffnet das Dialogfeld "Eigenschaften". Hier können Sie eine benutzerdefinierte Produktdefinition erstellen.

Informationen zum Produkt benutzerdefinierter Anfälligkeiten: Seite "Erkennungslogik"

Die nachstehenden Seiten beschreiben die Erkennungslogik, mit der die ausgewählte Erkennungsregel entscheidet, ob die Anfälligkeitsdefinition (oder ein anderer Definitionstyp) auf einem gescannten Gerät existiert.

Diese Dialogfelder entsprechen den Dialogfeldern der Erkennungslogik für heruntergeladene, bekannte Betriebssysteme und Anwendungsanfälligkeitsdefinitionen, die die o.g. Hersteller veröffentlicht haben. Weitere Informationen über die Optionen finden Sie in den entsprechenden Abschnitten oben.

Informationen zum Produkt benutzerdefinierter Anfälligkeiten: Seite "Erkennungslogik: Zur Erkennung verwendete Dateien"

Siehe oben Seite "Erkennungslogik: Zur Erkennung verwendete Dateien".

Informationen zum Produkt benutzerdefinierter Anfälligkeiten: Seite "Erkennungslogik: Zur Erkennung verwendete Registrierungseinstellungen".

Siehe oben Seite "Erkennungslogik: Zur Erkennung verwendete Registrierungseinstellungen".

Informationen zum Produkt benutzerdefinierter Anfälligkeiten: Seite "Erkennungslogik: Benutzerdefiniertes Erkennungsskript".

Siehe oben Seite "Erkennungslogik: Benutzerdefiniertes Skript".

Informationen zur Seite "Patchinformationen"

Verwenden Sie diese Seite, um die mit der Regel verknüpfte Patchdatei (sofern für die Reparatur erforderlich) und Logik zu definieren und zu konfigurieren, mit der ermittelt wird, ob das Patch bereits installiert ist. Sie können auch zusätzliche Patchdatei-Installations- oder Deinstallationsbefehle für benutzerdefinierte Reparaturen definieren.

Diese Seite und die ihr untergeordneten Seiten beziehen sich auf die Patchdatei, die zum Reparieren einer Anfälligkeit benötigt wird. Diese Seiten gelten nur, wenn die ausgewählte Erkennungsregel das Reparieren durch Bereitstellen einer Patchdatei zulässt. Wenn die Erkennungsregel sich auf das Scannen beschränkt oder der Sicherheitsinhaltstyp keine Patchdateien für die Reparatur einsetzt (dies ist z. B. bei Sicherheitsbedrohungen oder Spyware der Fall), sind diese Seiten nicht relevant.

- **Durch Patch repariert oder nur Erkennung:** Klicken Sie auf eine dieser Optionen, um anzugeben, ob die Erkennungsregel lediglich prüfen soll, ob die verknüpfte Definition existiert ("Nur erkennen"), oder ob sie die betreffende Definition auch reparieren soll, indem sie das vorgeschriebene Patch bereitstellt und installiert.
- **Patch-Downloadinformationen:**
    - **Patch-URL:** Zeigt den vollständigen Pfad und Dateinamen der Patchdatei an, die zum Reparieren der ausgewählten Definition benötigt wird. Der Speicherort, von dem aus die Patchdatei heruntergeladen wird.

- **Wird automatisch gedownloadet:** Gibt an, ob die Patchdatei automatisch von ihrem Hostserver heruntergeladen werden kann. Diese Option lässt sich mit benutzerdefinierten Erkennungsregeln verwenden, wenn Sie verhindern möchten, dass Patchdateien über das Kontextmenü der Regel heruntergeladen werden. Beispiel: Einen automatischen Patchdownload verhindern zu können, kann sich als notwendig erweisen, wenn eine Firewall existiert, die den Zugriff auf den Hostserver blockiert.
- **Download:** Wenn Sie eine benutzerdefinierte Erkennungsregel erstellen oder bearbeiten, die auch zur Reparatur verwendet wird, und Sie den Namen einer Patchdatei und eine URL eingegeben haben, können Sie auf **Downloaden** klicken, um zu versuchen, die Patchdatei jetzt herunterzuladen. Sie können die Patchdatei jedoch auch zu einem späteren Zeitpunkt downloaden.

- **Reparaturdaten:**
  - **Eindeutiger Dateiname:** Identifiziert den eindeutigen ausführbaren Dateinamen der Patchdatei.
    Beim Herunterladen einer Patchdatei wird dringend empfohlen, ein Hash für die Patchdatei zu erstellen, indem Sie auf **MD5-Hash generieren** klicken. (Die meisten, wenn nicht alle, Patchdateien bekannter Anfälligkeiten sollten ein Hash besitzen.) Die Patchdatei muss heruntergeladen werden, damit Sie ein Hash erstellen können. Eine Hash-Datei wird auch verwendet, um die Integrität der Patchdatei während der Reparatur (d. h., wenn die Patchdatei auf dem betroffenen Gerät bereitgestellt und installiert wird) zu gewährleisten. Der Sicherheitsscanner vergleicht hierfür den Hash-Code, den Sie beim Klicken auf die Schaltfläche "MD5-Hash erstellen" erstellt haben, mit dem neuen Hash, den er unmittelbar vor dem Versuch, die Patchdatei aus dem Patchrepository auf dem Gerät zu installieren, erstellt hat. Wenn die beiden Hash-Dateien identisch sind, wird der Reparaturvorgang fortgesetzt. Wenn die beiden Hash-Dateien nicht übereinstimmen, d. h. die Patchdatei seit dem Download in das Repository in irgendeiner Weise geändert wurde, wird der Reparaturvorgang eingestellt.
  - **Neustart erforderlich:** Gibt an, ob die Patchdatei einen Geräte-Neustart ausführen muss, bevor die Installations- und Konfigurationsprozesse auf dem Gerät abgeschlossen werden.
  - **Unbeaufsichtigte Installation:** Gibt an, ob die Installation der Patchdatei unbeaufsichtigt (ohne Beteiligung des Benutzers) abgeschlossen werden kann.

Die Seiten "Erkennung des Patches"

Die nachstehenden Seiten beziehen sich auf die Erkennungslogik, mit der die Regel prüft, ob das Patch bereits auf Geräten installiert ist.

WICHTIG: ALLE angegebenen Bedingungen für Dateien UND Registrierungseinstellungen müssen erfüllt sein, damit die Patchdatei als auf einem Gerät installiert erkannt wird.

Informationen zur Seite "Erkennung des Patches: Zur Erkennung installierter Patches verwendete Dateien".

Diese Seite spezifiziert die Dateibedingungen, mit deren Hilfe ermittelt wird, ob die Patchdatei bereits auf einem Gerät installiert ist. Die Optionen auf dieser Seite sind mit denen auf der Seite "Dateien" für die Definitionserkennungslogik identisch (siehe oben). Beim Erkennen von Patchinstallationen arbeitet die Logik jedoch umgekehrt. Das heißt, beim Suchen nach einer Patchinstallation müssen alle auf dieser Seite angegebenen Dateibedingungen erfüllt sein, damit eine Installation erkannt wird

Informationen zur Seite "Erkennung des Patches: Zur Erkennung installierter Patches verwendete Registrierungseinstellungen".

Diese Seite gibt die Registrierungsschlüssel-Bedingungen an, mithilfe derer ermittelt wird, ob die Patchdatei bereits auf einem Gerät installiert ist. Die Optionen auf dieser Seite sind mit denen auf der Seite "Registrierungseinstellungen" für die Definitionserkennungslogik identisch (siehe oben). In diesem Fall arbeitet die Logik jedoch umgekehrt. Das heißt, beim Suchen nach einer Patchinstallation müssen alle auf dieser Seite angegebenen Registrierungsbedingungen erfüllt sein, damit eine Installation erkannt wird

WICHTIG: ALLE angegebenen Bedingungen für Dateien UND Registrierungseinstellungen müssen erfüllt sein, damit die Patchdatei als auf einem Gerät installiert erkannt wird.

Seite zur Patchinstallation und -deinstallation

Mithilfe der nachstehenden Seiten können Sie zusätzliche Befehle konfigurieren, die ausgeführt werden, wenn das Patch auf betroffenen Geräten installiert oder deinstalliert wird.

Diese Option steht nur für benutzerdefinierte Definitionen zur Verfügung, die Reparaturvorgänge unterstützen.

Diese Befehle sind nützlich, wenn Sie konkrete Aktionen auf Zielgeräten programmieren müssen, um eine erfolgreiche Reparatur zu gewährleisten. Zusätzliche Befehle sind nicht erforderlich. Wenn Sie keine zusätzlichen Befehle konfigurieren, wird die Patchdatei standardmäßig für sich allein ausgeführt. Denken Sie daran, dass Sie beim Konfigurieren zusätzlicher Befehle auch einen Befehl integrieren müssen, der die eigentliche Patchdatei mit dem Befehl "Ausführen" ausführt.

Informationen zur Seite "Patchinstallationsbefehle"

Verwenden Sie diese Seite zum Konfigurieren zusätzlicher Befehle für Patchinstallationstasks. Die verfügbaren Befehle sind für die Patchinstallation und -deinstallation identisch.

- **Befehle:** Listet Befehle in der Reihenfolge ihrer Ausführung auf Zielgeräten auf. Wählen Sie einen Befehl aus, um seine Argumente anzuzeigen. Sie können die Befehlsreihenfolge mithilfe der Schaltflächen **Nach oben** und **Nach unten** ändern. Um einen Befehl aus der Liste zu entfernen, wählen Sie ihn aus und klicken auf **Entfernen**.
- **Hinzufügen:** Öffnet ein Dialogfeld, in dem Sie einen Befehlstyp für die Liste "Befehle" auswählen können.
- **Befehlsargumente:** Zeigt die Argumente an, die den ausgewählten Befehl definieren. Die Werte eines Arguments können bearbeitet werden. Sie können jedes Argument bearbeiten, indem Sie auf das Feld **Wert** des betreffenden Arguments doppelklicken und dann direkt in das Feld schreiben. Bei allen Befehlstypen können Sie auch mit der rechten Maustaste in das Feld **Wert** klicken, um einen Makro/eine Variable in das Argument einzufügen.

Die folgende Liste beschreibt die Befehle und ihre Argumente:

- **Kopieren:** Kopiert eine Datei aus der angegebenen Quelle in das angegebene Ziel auf der Festplatte des Zielgeräts. Diese Befehle können vor und/oder nach der Ausführung des tatsächlichen Patch ausgeführt werden. Beispiel: Nachdem Sie den Inhalt einer komprimierten Datei mit dem Unzip-Befehl extrahiert haben, möchten Sie Dateien von einem Speicherort in einen anderen kopieren.

  Die Argumente für den Kopierbefehl lauten: Ziel (Pfad, in den Sie die Datei kopieren möchten, ausschließlich des Dateinamens) und Quelle (vollständiger Pfad und Dateiname der Datei, die Sie kopieren möchten).

- **Ausführen:** Führt die Patchdatei oder jede andere ausführbare Datei auf den Zielgeräten aus.

Die Argumente für den Ausführungsbefehl lauten: Pfad (vollständiger Pfad und Dateiname des Speicherortes, an dem sich die ausführbare Datei befindet; für die Patchdatei können Sie die Variablen %SDMCACHE% und %PATCHFILENAME% verwenden), Args (Befehlszeilenoptionen für die ausführbare Datei; beachten Sie, dass dieses Feld kein erforderliches Feld ist), Timeout (Anzahl von Sekunden, die bis zur vollständigen Ausführung der ausführbaren Datei abgewartet werden soll, bevor der Vorgang mit dem nächsten Befehl in der Liste fortgesetzt wird – gilt, wenn für das Argument "Wait" die Einstellung "Wahr" gewählt wurde) und Wait ("Wahr"- oder "Falsch"-Wert, der festlegt, ob die vollständige Ausführung der ausführbaren Datei abgewartet werden soll, bevor der Vorgang mit dem nächsten Befehl in der Liste fortgesetzt wird).

- **ButtonClick:** Klickt automatisch auf eine angegebene Schaltfläche, die während der Ausführung einer ausführbaren Datei angezeigt wird. Mit diesem Befehl können Sie einen Schaltflächen-Mausklick programmieren, sofern eine solche Interaktion von der ausführbaren Datei verlangt wird.

  Damit "ButtonClick" ordnungsgemäß funktioniert, muss das Argument "Wait" für den vorhergehenden Ausführungsbefehl auf "falsch" gesetzt werden. Mit dieser Vorgehensweise stellen Sie sicher, dass die ausführbare Datei vor dem Weitermachen mit der Klick-Aktion auf die Schaltfläche nicht beendet werden muss.

  Die Argumente für den ButtonClick-Befehl lauten: Erforderlich (der Wert "wahr" oder "falsch" gibt an, ob die Schaltfläche angeklickt werden muss, damit der Vorgang fortgesetzt werden kann; wenn Sie "wahr" auswählen und die Schaltfläche sich aus irgendeinem Grund nicht anklicken lässt, wird die Reparatur fortgesetzt), ButtonIDorCaption (benennt die anzuklickende Schaltfläche anhand ihres Text-Labels oder ihrer Control-ID), Timeout (Anzahl von Sekunden, die die anzuklickende Schaltfläche während der Ausführung der ausführbaren Datei eingeblendet wird) und WindowCaption (benennt das Fenster oder Dialogfeld, in dem sich die anzuklickende Schaltfläche befindet).

- **ReplaceInFile:** Bearbeitet eine textbasierte Datei auf Zielgeräten. Verwenden Sie diesen Befehl, wenn Sie vor oder nach dem Ausführen der Patchdatei Änderungen in einer textbasierten Datei vornehmen müssen (beispielsweise Änderung eines bestimmten Wertes in einer .INI-Datei), um sicherzustellen, dass die Datei korrekt ausgeführt wird.

  Die Argumente für den ReplaceInFile-Befehl lauten: Dateiname (vollständiger Pfad und Name der Datei, die Sie bearbeiten möchten), ReplaceWith (exakte Textzeichenfolge, die Sie zur Datei hinzufügen möchten) und Original Text (exakte Textzeichenfolge, die Sie in der Datei ersetzen möchten).

- **StartService:** Startet einen Dienst auf Zielgeräten. Verwenden Sie diesen Befehl, um einen Dienst zu starten, der benötigt wird, um die Patchdatei ausführen zu können, oder um einen Dienst neu zu starten, der zuvor gestoppt werden musste, damit die Patchdatei ausgeführt werden konnte.

  Die Argumente für den StartService-Befehl lauten: Dienst (Name des Dienstes).

- **StopService:** Stoppt einen Dienst auf Zielgeräten. Verwenden Sie diesen Befehl, wenn ein Dienst auf einem Gerät gestoppt werden muss, damit die Patchdatei installiert werden kann.

  Die Argumente für den StopService-Befehl lauten: Dienst (Name des Dienstes).

- **Unzip:** Entzippt eine komprimierte Datei auf Zielgeräten. Sie können diesen Befehl beispielsweise verwenden, wenn die Reparatur die Ausführung oder das Kopieren mehrerer Dateien auf die Zielgeräten erforderlich macht.

  Die Argumente für den Unzip-Befehl lauten: Ziel (vollständiger Pfad, in dem Sie den Inhalt einer komprimierten Datei auf der Festplatte eines Geräts extrahieren möchten) und Quelle (vollständiger Pfad und Dateiname der komprimierten Datei).

- **WriteRegistryValue:** Schreibt einen Wert in die Registrierung.

  Die Argumente für WriteRegistryValue lauten: Key, Type, ValueName, ValueData, WriteIfDataEmpty

Informationen zur Seite "Patchdeinstallationsbefehle"

Verwenden Sie diese Seite zum Konfigurieren zusätzlicher Befehle für Patchdeinstallationstasks. Die verfügbaren Befehle sind für die Patchinstallation und -deinstallation identisch. Auf der Seite "Patchdeinstallationsbefehle" stehen jedoch zwei spezielle Optionen zur Verfügung:

- **Patch kann deinstalliert werden:** Gibt an, ob die Patchdatei auf reparierten Geräten deinstalliert werden kann.
- **Für die Deinstallation wird das Original-Patch benötigt:** Gibt an, ob auf die eigentliche ausführbare Datei des Original-Patch auf dem Coreserver Zugriff bestehen muss, damit das Patch auf den gescannten Geräten deinstalliert werden kann.

Informationen zu den Befehlen finden Sie unter "Informationen zur Seite "Patchinstallationsbefehle"" auf Seite 668.

Informationen zum Dialogfeld "Verknüpfte Patches downloaden"

Dieses Dialogfeld verwenden Sie, um ausführbare Patchdateien herunterzuladen, die zum Reparieren der ausgewählten Anfälligkeit benötigt werden, jedoch gegenwärtig weder auf dem Coreserver (noch in einem anderen angegebenen Patchrepository) zur Verfügung stehen. Die für eine Reparatur benötigten Patches müssen in dem zugewiesenen Patchspeicherort gespeichert sein, damit ein verwaltetes Gerät, auf dem eine Anfälligkeit erkannt wurde, repariert werden kann.

- **Name:** Gibt den Namen der ausführbaren Patchdatei an.
- **Definitionen:** Gibt die Anfälligkeit an, mit der diese Patchdatei verbunden ist.
- **Gedownloadet:** Gibt an, ob die Patchdatei heruntergeladen wurde oder nicht.
- **Kann downloaden:** Gibt an, ob das Patch automatisch heruntergeladen werden kann oder ob es durch einen Patch und Compliance-Prozess heruntergeladen werden muss.
- **Nur aktuell benötigte Patches anzeigen:** Zeigt nur diejenigen Patchdateien an, die benötigt werden, um die ausgewählte Anfälligkeit zum gegenwärtigen Zeitpunkt zu reparieren. Mit anderen Worten: Die Liste umfasst Patches, die ältere Patches ersetzt haben, jedoch nicht die älteren Patches.
- **Alle verknüpften Patches anzeigen:** Zeigt eine umfassende Liste aller zugehörigen Patches für die ausgewählte Anfälligkeit an, unabhängig davon, ob einzelne Patches zwischenzeitlich ersetzt wurden oder nicht.
- **Download:** Klicken Sie, um die Patchdateien aus der Updatequelle herunterzuladen.
- **Abbrechen:** Storniert den Downloadvorgang.

Hilfe zu Patch- und Compliancetasks

Informationen zum Dialogfeld "Sicherheitsscantask erstellen"

Dieses Dialogfeld verwenden Sie, um einen geplanten Task zu erstellen und zu konfigurieren, der einen Sicherheitsscanner auf Zielgeräten ausführt.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers " erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" (für Sicherheits- und Compliancescantasks und Reparaturtasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Sie können auch einen sofortigen On-Demand-Sicherheits- und Compliancescan auf einem oder mehreren Zielgeräten veranlassen. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät (oder auf bis zu 20 gleichzeitig ausgewählte Geräte), klicken Sie auf **Sicherheitsscan**, wählen Sie Scan- und Reparatureinstellungen aus oder klicken Sie auf **Compliancescan** und klicken Sie dann auf **OK**.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Geben Sie einen eindeutigen Namen zur Identifizierung des Sicherheitsscantasks ein.
- **Geplanten Task erstellen:** Fügt den Sicherheitsscantask zum Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Richtlinie erstellen:** Fügt den Sicherheitsscantask als Richtlinie zum Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **Scan- und Reparatureinstellungen:** Gibt an, welche Scan- und Reparatureinstellungen für den Scantask verwendet wurden. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten, wie sich die Interaktion mit den Benutzern gestaltet und welche Sicherheitsinhalte gescannt werden. Wählen Sie Scan- und Reparatureinstellungen aus der Dropdownliste aus, um sie dem Sicherheitsscantask hinzuzufügen, die Sie gerade erstellen. Sie können auf **Bearbeiten** klicken, um die Optionen für die ausgewählten Scan- und Reparatureinstellungen zu ändern. Sie können auch auf **Konfigurieren** klicken, um neue Scan- und Reparatureinstellungen zu erstellen.

Informationen zum Dialogfeld "Compliancescantask erstellen"

Dieses Dialogfeld verwenden Sie zum Erstellen und Konfigurieren eines Tasks, der den Sicherheitsscanner ausführt, um Zielgeräte speziell auf Konformität mit Ihrer Sicherheitsrichtlinie (basierend auf dem Inhalt der Gruppe "Compliance") zu überprüfen.

HINWEIS: On-demand-Sicherheits- und Compliancescans
Sie können auch einen sofortigen Sicherheits- oder Compliancescan auf einem oder mehreren Zielgeräten veranlassen. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät (oder auf bis zu 20 gleichzeitig ausgewählte Geräte), klicken Sie auf **Sicherheitsscan**, wählen Sie Scan- und Reparatureinstellungen aus oder klicken Sie auf **Compliancescan** und klicken Sie dann auf **OK**.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Hier geben Sie einen eindeutigen Namen für den Compliancescantask ein.
- **Geplanten Task erstellen:** Fügt den Compliancescantask zum Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Zielcomputer, die seit folgendem Datum keine Ergebnisse gemeldet haben:** Begrenzt den Compliancescan auf diejenigen verwalteten Geräte, die seit dem von Ihnen angegebenen Datum keine Sicherheitsscan-Ergebnisse gemeldet haben.
- **Jetzt starten:** Legt fest, dass der geplante Scantask auszuführen ist, sobald er dem Fenster "Geplante Tasks" hinzugefügt wurde. Damit ersparen Sie sich das manuelle Konfigurieren von Zeitplanoptionen.
- **Richtlinie erstellen:** Fügt den Compliancetask als Richtlinie dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.

Informationen zum Dialogfeld "Task - Einstellungen ändern"

Dieses Dialogfeld verwenden Sie, um einen Task zu erstellen und zu konfigurieren, der die Standardeinstellungen auf Zielgeräten für Patch und Compliance-Dienste ändert. Hierzu zählen die folgenden Einstellungen:

- Scan- und Reparatureinstellungen
- Compliance-Sicherheitseinstellungen (gilt nur für Compliance-Sicherheitsscans)
- Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen

Mit einem Einstellungsänderungstask lassen sich die Standardeinstellungen eines Geräts (die in die lokale Registrierung des Geräts geschrieben werden) bequem ändern, ohne erneut eine vollständige Agentenkonfiguration bereitstellen zu müssen.

- **Taskname:** Geben Sie zur Identifizierung des Tasks einen eindeutigen Namen ein.
- **Geplanten Task erstellen:** Fügt den Task dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Richtlinie erstellen:** Fügt den Task als Richtlinie dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **Scan- und Reparatureinstellungen:** Legt die für Sicherheitsscantasks zu verwendenden Scan- und Reparatureinstellungen fest. Die Scan- und Reparatureinstellungen legen fest, ob der Scanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten, wie sich die Interaktion mit den Benutzern gestaltet und welche Sicherheitsinhalte gescannt werden. Wählen Sie eine der Einstellungen aus der Dropdownliste aus. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählten Einstellungen zu ändern. Klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen. Weitere Informationen finden Sie unter "Informationen zu den Dialogfeldseiten "Scan- und Reparatur- (und Compliance-)Einstellungen"" auf Seite 678.
- **Compliance-Einstellungen:** Gibt Compliance-Einstellungen an, die für Compliancescantasks verwendet werden. Mit den Compliance-Einstellungen legen Sie fest, wann und wie ein Compliancescantask durchgeführt wird, ob die Reparatur automatisch zu erfolgen hat und/oder was zu tun ist, wenn LANDesk Antivirus einen Virenbefall auf Zielgeräten diagnostiziert.

- **Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen:** Gibt Einstellungen für die Außerkraftsetzung von benutzerdefinierten Variablen auf Zielgeräten an, wenn diese auf Sicherheitsdefinitionen durchsucht werden, die benutzerdefinierte Variablen enthalten (beispielsweise Sicherheitsbedrohungen und Viren). Mithilfe der Funktion "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen" können Sie Einstellungswerte angeben, die Sie während eines Sicherheitsscans ignorieren oder umgehen möchten. Dies ist eine äußerst nützliche Funktion, wenn Sie ein gescanntes Gerät NICHT als anfällig in Übereinstimmung mit den standardmäßigen benutzerdefinierten Variableneinstellungen identifizieren lassen möchten. Wählen Sie eine der Einstellungen aus der Dropdownliste aus. Über die Dropdownliste können Sie außerdem veranlassen, dass die Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen auf Zielgeräten entfernt werden. Mit der Option **Benutzerdefinierte Variableneinstellungen entfernen** können Sie die Einstellungen auf einem Gerät so festlegen, dass benutzerdefinierte Variableneinstellungen vollständig in Kraft sind. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählten Einstellungen zu ändern. Klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen. Weitere Informationen hierzu finden Sie unter "Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen"" auf Seite 685.

Informationen zum Dialogfeld "Neustarttask erstellen"

Dieses Dialogfeld verwenden Sie zum Erstellen und Konfigurieren eines allgemeinen Neustarttasks.

Ein Neustarttask ist eine nützliche Funktion, wenn Sie Patches (ohne Neustart) als einzelnen Prozess installieren und dann die auf diese Weise reparierten Geräte in einem separaten Task neu starten möchten. Beispiel: Sie können einen Scan- oder Patchinstallationstask tagsüber und dann einen reinen Neustarttask zu einer für die Endbenutzer günstigeren Uhrzeit ausführen lassen.

- **Taskname:** Kennzeichnet den Task mit einem eindeutigen Namen.
- **Geplanten Task erstellen:** Erstellt einen Neustart-Task im Fenster "Geplante Tasks", wenn Sie auf **OK** klicken.
- **Richtlinie erstellen:** Erstellt eine Neustartrichtlinie, wenn Sie auf **OK** klicken.
- **Scan- und Reparatureinstellungen:** Gibt an, welche Neustartkonfiguration aus den Scan- und Reparatureinstellungen verwendet wird, damit der Task Neustartanforderungen und auf den Zielgeräten auszuführende Aktionen bestimmen kann. Wählen Sie Scan- und Reparatureinstellungen aus der Dropdownliste aus oder klicken Sie auf **Konfigurieren**, um neue Scan- und Reparatureinstellungen zu definieren.

Informationen zum Dialogfeld "Reparaturtask erstellen"

Dieses Dialogfeld verwenden Sie zum Erstellen und Konfigurieren eines Reparaturtasks (Remediationtasks) für folgende Definitionstypen: Anfälligkeiten, Spyware, LANDesk Softwareupdates, benutzerdefinierte Definitionen und Sicherheitsbedrohungen mit zugehörigem Patch. Die Option "Reparatur planen" gilt nicht für blockierte Anwendungen.

Dieses Dialogfeld umfasst die folgenden Seiten:

- "Informationen zum Dialogfeld "Reparaturtask erstellen": Seite "Allgemein"" auf Seite 673
- "Informationen zum Dialogfeld "Reparaturtask erstellen": Seite "Patches"" auf Seite 674

Informationen zum Dialogfeld "Reparaturtask erstellen": Seite "Allgemein"

- **Taskname:** Kennzeichnet den Reparatur-Task mit einem eindeutigen Namen. Standardmäßig wird der Name der ausgewählten Definition oder der benutzerdefinierten Gruppe verwendet. Sie können diesen Namen nach Bedarf bearbeiten.

- **Als geplanten Task reparieren:** Erstellt einen Sicherheits-Reparaturtask im Fenster "Geplante Tasks", wenn Sie auf **OK** klicken.
- **In Staging- und Reparaturtask teilen:** (Optional) Hiermit können Sie im Tool "Geplante Tasks" zwei getrennte Tasks erstellen; einen für die Bereitstellung der erforderlichen Patchdateien im lokalen Cache des Zielgeräts, und einen zweiten für die eigentliche Installation dieser Patchdateien auf den betroffenen Geräten.
    - **Computer zum Reparieren auswählen:** Gibt an, welche Geräte zur geplanten Reparatur hinzugefügt werden sollen. Sie können "Keine Geräte", "Alle betroffenen Geräte" (Geräte, auf denen die Definition vom letzten Sicherheitsscan erkannt wurde) oder nur die "Betroffenen Geräte, die auch ausgewählt sind" auswählen (letztere Option ist nur verfügbar, wenn Sie vom Dialogfeld "Security- und Patchinformationen" eines Geräts auf das Dialogfeld "Reparatur planen" zugreifen).
    - **Multicast verwenden:** Aktiviert Targeted Multicast für die Patchbereitstellung auf Geräten. Klicken Sie auf diese Option und auf **Multicast-Optionen**, wenn Sie Multicast-Optionen konfigurieren möchten. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "Multicastoptionen"" auf Seite 674.
- **Als Richtlinie reparieren:** Erstellt eine Sicherheits-Reparaturrichtlinie, wenn Sie auf **OK** klicken.
    - **Abfrage hinzufügen, die betroffene Geräte repräsentiert:** Erstellt eine neue Abfrage auf der Basis der ausgewählten Definition und überträgt sie auf die Richtlinie. Diese abfragebasierte Richtlinie sucht nach Geräten, die von der ausgewählten Definition betroffen sind, und stellt das entsprechende Patch bereit.
    - **Patch nur von lokalen Peers downloaden:** Beschränkt die Patchbereitstellung derart, dass diese nur dann stattfindet, wenn sich die Patchdatei im lokalen Cache des Geräts oder auf einem Peer im gleichen Subnetz befindet. Mit dieser Option lässt sich Netzwerkbandbreite sparen; beachten Sie jedoch, dass die Patchdatei sich aktuell an einem dieser beiden Orte befinden muss, damit die Patchinstallation erfolgreich ausgeführt werden kann.
    - **Patch nur downloaden (nicht reparieren):** Lädt die Patchdatei in das Patchrepository, stellt es aber nicht bereit. Sie können diese Option verwenden, wenn Sie die Patchdatei vor der eigentlichen Bereitstellung in einem mehrstufigen Szenarium zu Testzwecken abrufen möchten.
- **Scan- und Reparatureinstellungen:** Gibt an, welche Scan- und Reparatureinstellungen für den Reparaturtask verwendet werden. Damit wird entschieden, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird. Wählen Sie Scan- und Reparatureinstellungen aus der Dropdownliste aus oder klicken Sie auf **Konfigurieren**, um neue Scan- und Reparatureinstellungen zu definieren.

Informationen zum Dialogfeld "Reparaturtask erstellen": Seite "Patches"

Diese Seite verwenden Sie, um entweder nur benötigte Patches oder alle assoziierten Patches für die ausgewählte Anfälligkeit aufzuführen. (**HINWEIS:** Die Felder auf dieser Seite sind dieselben wie die unter "Informationen zum Dialogfeld "Verknüpfte Patches downloaden"" auf Seite 670.)

Wenn Sie Patches direkt von dieser Seite downloaden möchten (sofern diese noch nicht im Patchrepository platziert wurden), klicken Sie auf **Downloaden**.

Informationen zum Dialogfeld "Multicastoptionen"

Dieses Dialogfeld verwenden Sie, um die folgenden Targeted Multicast-Optionen für einen geplanten Sicherheitsreparaturtask zu konfigurieren:

- **Multicast-Domänenerkennung:**
  - **Multicast-Domänenerkennung verwenden:** Wählen Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen. Bei dieser Option werden die Domänenerkennungsergebnisse für die erneute Verwendung nicht gespeichert.
  - **Multicast-Domänenerkennung verwenden und Ergebnisse speichern:** Wählen Sie diese Option, wenn Sie Targeted Multicast verwenden möchten, um eine Domänenerkennung für diesen Auftrag durchzuführen und die Ergebnisse für eine künftige Verwendung zu speichern; somit sparen Sie Zeit bei folgenden Multicasts.
  - **Ergebnisse der letzten Multicast-Domänenerkennung verwenden:** Verwenden Sie diese Option immer dann, wenn Sie durch Targeted Multicast eine Domänenerkennung durchgeführt und die Ergebnisse gespeichert haben.
- **Domänenrepräsentanten zum Reaktivieren von Computern verwenden:** Verwenden Sie diese Option, wenn Sie Computer, die die "Wake On Lan"-Technologie unterstützen, beim Empfang von Multicast reaktivieren möchten.
- **Wartezeit in Sekunden nach Wake on LAN:** Legt fest, wie lange Domänenrepräsentanten auf das Multicast warten, nachdem das Wake On LAN-Paket gesendet wurde. Die Standardwartezeit beträgt 120 Sekunden. Wenn Computer im Netzwerk länger als 120 Sekunden zum Starten benötigen, sollten Sie diesen Wert erhöhen. Der zulässige Höchstwert liegt bei 3600 Sekunden (eine Stunde).

Mit den nachfolgenden Optionen können Sie Task-spezifische Targeted Multicast-Parameter konfigurieren. Die Standardwerte sind in der Regel für die meisten Multicasts geeignet. Auswirkungen der Optionen:

- **Höchstzahl gleichzeitig arbeitender Multicast-Domänenrepräsentanten:** Die Zahl der Repräsentanten, die aktiv zur selben Zeit einen Multicast durchführen, ist auf diese Anzahl beschränkt.
- **Verarbeitung von Rechnern einschränken, bei denen Multicast fehlschlug:** Wenn ein Gerät die Datei über Multicast nicht erhält, lädt es die Datei von der Website oder vom Dateiserver herunter. Dieser Parameter kann verwendet werden, um die Anzahl der Geräte zu beschränken, die die Datei gleichzeitig erhalten. Wenn z. B. die Höchstanzahl von Threads 200 war und die Höchstanzahl der fehlgeschlagenen Multicast-Threads bei 20 lag, würden im Dialogfeld "Benutzerdefinierte Tasks" nicht mehr als 20 Computer gleichzeitig verarbeitet werden, bei denen Multicast fehlgeschlagen ist. Das Dialogfeld "Benutzerdefinierte Tasks" verarbeitet bis 200 Geräte gleichzeitig, wenn diese erfolgreich den Multicast erhalten haben. Es verarbeiten jedoch nur maximal 20 der 200 Threads Geräte, bei denen der Multicast-Task misslungen ist. Wenn dieser Wert auf 0 festgelegt ist, führt das Dialogfeld "Benutzerdefinierte Tasks" den Verteilungsabschnitt des Task für keinen der Computer durch, auf dem das Multicasting fehlgeschlagen ist.
- **Anzahl von Tagen, die die Dateien im Cache verbleiben:** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache des jeweiligen Zielcomputers gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Anzahl von Tagen, die die Dateien im Cache des Multicast-Domänenrepräsentanten verbleiben:** Die Zeitspanne, die die Datei, für die das Multicasting durchgeführt wird, im Cache auf dem Multicast-Domänenrepräsentanten gespeichert wird. Nach Ablauf dieser Zeitspanne wird die Datei automatisch gelöscht.
- **Minimale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Mindestwartezeit zwischen dem Senden von Multicast-Paketen.

Dieser Wert wird nur verwendet, wenn der Domänenrepräsentant kein Multicasting einer Datei aus dem eigenen Cache durchführt. Wenn dieser Parameter nicht festgelegt wird, wird die auf dem Subnetz/Domänenrepräsentantencomputer gespeicherte Mindestruhezeit verwendet. Sie können mithilfe dieses Parameters die Bandbreitennutzung im WAN beschränken.

- **Maximale Zahl von Millisekunden zwischen Paketübertragungen (WAN oder Lokal):** Höchstwartezeit zwischen dem Senden von Multicast-Paketen. Weitere Informationen finden Sie weiter oben unter "Mindestzahl in Millisekunden zwischen Paketübertragungen".

Informationen zum Dialogfeld "Patch deinstallieren"

Dieses Dialogfeld verwenden Sie, um einen Deinstallationstask für Patches zu erstellen und zu konfigurieren, die auf betroffenen Geräten bereitgestellt wurden

- **Taskname:** Kennzeichnet den Task mit einem eindeutigen Namen. Standard ist der Name des Patch. Sie können diesen Namen nach Bedarf bearbeiten.
- **Als geplanten Task deinstallieren:** Erstellt einen Task für eine Patchdeinstallation im Fenster "Geplante Tasks", wenn Sie auf **OK** klicken.
    - **Ziele auswählen:** Gibt an, welche Geräte zum Task für die Patchdeinstallation hinzugefügt werden sollen. Sie können "keine Geräte", "alle Geräte, auf denen das Patch installiert ist" oder "nur die Geräte, auf denen das Patch installiert und die auch ausgewählt sind" auswählen (diese letzte Option ist nur verfügbar, wenn Sie vom Dialogfeld "Sicherheits- und Patchinformationen" eines Geräts auf das Dialogfeld "Patch deinstallieren" zugreifen).
- **Wenn das Original-Patch erforderlich ist:**
    - **Multicast verwenden:** Aktiviert Targeted Multicast für die Bereitstellung des Patchdeinstallationstasks auf Geräten. Klicken Sie auf diese Option und klicken Sie auf **Multicast-Optionen**, wenn Sie Multicast-Optionen konfigurieren möchten. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "Multicastoptionen"" auf Seite 674.
- **Als Richtlinie deinstallieren:** Erstellt eine Richtlinie für eine Patchdeinstallation im Fenster "Geplante Tasks", wenn Sie auf **OK** klicken.
    - **Abfrage hinzufügen, die betroffene Geräte repräsentiert:** Erstellt eine neue Abfrage auf der Basis des ausgewählten Patch und überträgt sie auf die Richtlinie. Diese abfragebasierte Richtlinie sucht nach Geräten, auf denen das ausgewählte Patch installiert ist, und deinstalliert es.
- **Scan- und Reparatureinstellungen:** Gibt an, welche Scan- und Reparatureinstellungen für den Deinstallationstask verwendet werden. Die Einstellungen legen fest, ob der Sicherheitsscanner auf Geräten angezeigt wird, definiert Neustartoptionen, MSI-Speicherortinformationen etc. Wählen Sie Scan- und Reparatureinstellungen aus der Dropdownliste aus oder klicken Sie auf **Konfigurieren**, um neue Scan- und Reparatureinstellungen zu definieren.

Informationen zum Dialogfeld "Vergangenheitsdaten erfassen"

Dieses Dialogfeld verwenden Sie, um Daten zu gescannten und erkannten Anfälligkeiten auf verwalteten Geräten zu erfassen. Diese Informationen finden in Sicherheitsberichten Verwendung. Sie können die Daten entweder sofort oder mithilfe eines Tasks während einer bestimmten Zeitspanne erfassen.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Kennzeichnet den Task "Vergangenheitsdaten aufzeichnen" mit einem eindeutigen Namen.

- **Vergangenheitsdaten speichern für:** Gibt an, für welchen Zeitraum (in Tagen) Daten erfasst werden. Sie können 1 bis 3.000 Tage angegeben.
- **Berichtsdaten zu Definitionen generieren, deren Veröffentlichung weniger als ... zurückliegt:** Beschränkt den Bericht auf Daten zu Anfälligkeiten, die innerhalb des angegebenen Zeitraums veröffentlicht wurden.
- **Warnen:** Zeigt auf der Coreserverkonsole eine Meldung an, wenn ein Task zur Erfassung von Vergangenheitsdaten nicht innerhalb des angegebenen Zeitraums ausgeführt wurde.
- **Jetzt sammeln:** Sammelt sofort die aktuellen Daten zu erkannten, gescannten und nicht gescannten Anfälligkeiten.
- **Task erstellen:** Fügt den Task dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Entfernen:** Entfernt alle bisher zu Anfälligkeiten erfassten Daten.

Hilfe zu Patch und Compliance-Einstellungen

Informationen zum Dialogfeld "Scan- und Reparatur- (und Compliance-) Einstellungen konfigurieren"

Dieses Dialogfeld verwenden Sie, um Ihre Scan-, Reparatur- (und Compliance-)Einstellungen zu verwalten. Nachdem Sie die Einstellungen konfiguriert haben, können Sie sie auf Sicherheits- und Compliancescantasks sowie auf Reparatur-, Deinstallations- und Neustarttasks anwenden.

Dieses Dialogfeld enthält folgende Optionen:

- **Neu:** Öffnet das Dialogfeld "Einstellungen". Hier können Sie die Optionen bzgl. des angegebenen Einstellungstyps konfigurieren.
- **Bearbeiten:** Öffnet das Dialogfeld "Einstellungen". In diesem Dialogfeld können Sie die ausgewählten Einstellungen bearbeiten.
- **Kopieren:** Öffnet eine Kopie der ausgewählten Einstellungen als Vorlage, die von Ihnen dann bearbeitet und umbenannt werden können.
- **Löschen:** Entfernt die ausgewählten Einstellungen aus der Datenbank.

  HINWEIS: Die ausgewählten Einstellungen sind zur Zeit möglicherweise mit Tasks oder verwalteten Geräten verknüpft. Wenn Sie diese Einstellungen löschen, verfügen Geräte mit diesen Einstellungen weiterhin über diese Einstellungen und verwenden diese auch nach wie vor, bis ein neuer Task vom Typ "Einstellungen ändern" bereitgestellt wird; geplante Tasks, die über diese Einstellungen verfügen, werden weiterhin auf Zielgeräten ausgeführt, genauso wie Local Scheduler-Tasks, die über diese Einstellungen verfügen. Auch sie werden solange ausgeführt, bis eine neue Konfiguration bereitgestellt wird.

- **Schließen:** Schließt das Dialogfeld, ohne Einstellungen auf den Task anzuwenden.

Informationen zu den Dialogfeldseiten "Scan- und Reparatur- (und Compliance-) Einstellungen"

Dieses Dialogfeld verwenden Sie, um Scan- und Reparatureinstellungen zu erstellen und zu bearbeiten. Die Scan- und Reparatureinstellungen legen fest, ob der Sicherheitsscanner während der Ausführung auf Geräten angezeigt wird, welche Neustartoptionen gelten, wie sich die Interaktion mit den Benutzern gestaltet und welche Sicherheitsinhalte gescannt werden.

HINWEIS: Hinweise zu den Compliancescan-Einstellungen
Die Informationen in diesem Dialogfeld können auch auf Compliancescans angewendet werden, wobei die Seite **Compliance** die Funktion der Seite **Scannen** übernimmt. Weitere Informationen zu den relevanten Einstellungen für Compliancescans finden Sie weiter unten im Abschnitt "Informationen zur Seite 'Compliance'".

HINWEIS: Hinweise zu den Einstellungen für den Neustarttask
Die Einstellungen auf der Seite **Neu starten** dieses Dialogfelds können auch für einen Task vom Typ "Nur neu starten" verwendet werden.

Sie können beliebig viele Scan- und Reparatureinstellungen definieren und diese jederzeit bearbeiten. Beispiel: Sie können für Scan- und Reparatureinstellungen eine besondere Benachrichtigungs- und Neustartbedingung für Desktopgeräte und eine weitere für unterschiedliche Server-Neustartoptionen konfigurieren. Sie können aber auch Scan- und Reparatureinstellungen für das Scannen auf Windows-Anfälligkeiten und andere für das Scannen auf Spyware konfigurieren etc.

Nachdem Sie Scan- und Reparatureinstellungen konfiguriert haben, können Sie sie auf Sicherheitsscan-Tasks, Reparaturtasks, Deinstallationstasks und Tasks für den Neustart von Geräten anwenden.

Scan- und Reparatureinstellungen

- **Name:** Kennzeichnet die Einstellungen mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Einstellungen" in einem Sicherheitstask-Dialogfeld angezeigt.

Das Dialogfeld "Einstellungen" umfasst die folgenden Seiten:

- "Informationen zur Seite "Allgemeine Einstellungen"" auf Seite 678
- "Informationen zur Seite "Scanoptionen"" auf Seite 679
- "Informationen zur Seite "Compliance-Einstellungen"" auf Seite 680
- "Informationen zur Seite "Reparaturoptionen"" auf Seite 681
- "Informationen zur Seite "MSI-Informationen"" auf Seite 682
- "Informationen zur Seite "Neustartoptionen"" auf Seite 682
- "Informationen zur Seite "Netzwerkeinstellungen"" auf Seite 683
- "Informationen zur Seite "Pilotkonfiguration"" auf Seite 683
- "Informationen zur Seite "Spyware-Scannen"" auf Seite 683

Informationen zur Seite "Allgemeine Einstellungen"

- **Fortschrittsdialog anzeigen:** Ermöglicht es dem Sicherheitsscanner, während der Ausführung auf Endbenutzergeräten Informationen einzublenden. Wählen Sie eine Option aus der Dropdownliste aus (Niemals, Immer, Nur bei Reparatur), um festzulegen, ob und wann Scanneraktivität angezeigt wird und ob Sie andere Anzeige- und Interaktionsoptionen in diesem Dialogfeld konfigurieren möchten. Wenn Sie "Niemals" auswählen, wird keine der anderen Optionen auf dieser Seite für den

Konfigurationsvorgang zur Verfügung gestellt und der Scanner wird transparent auf Geräten ausgeführt. Wenn Sie "Immer" auswählen, können Sie die anderen Optionen konfigurieren.

- **Ausblenden, wenn der Benutzer gerade eine Präsentation zeigt:** Sorgt dafür, dass der Sicherheitsscanner nicht auf Endbenutzergeräten angezeigt wird, auf denen gerade die Anwendung Microsoft Office PowerPoint ausgeführt wird.
- **Benutzer darf Scan abbrechen:** Blendet die Schaltfläche "Abbrechen" im Dialogfeld des Sicherheitsscanners auf dem Gerät des Endbenutzers ein. Klicken Sie auf diese Option, wenn Sie dem Endbenutzer die Möglichkeit geben möchten, einen Scan abzubrechen. Wenn diese Option nicht aktiviert ist, enthält das Dialogfeld keine Schaltfläche zum Abbrechen, sodass der Endbenutzer den Scan nicht stoppen kann.
- **Wenn kein Neustart erforderlich ist:**
  - **Endbenutzereingabe vor Abschluss des Vorgangs anfordern:** Bei einem Scan, der ohne Neustart vollständig ausgeführt werden kann, klicken Sie auf diese Option, wenn der Scanner eine Abfrage für den Endbenutzer einblenden soll, bevor das Anzeige-Dialogfeld des Scanners auf dem Gerät geschlossen wird. Wenn Sie diese Option auswählen und der Endbenutzer nicht reagiert, bleibt das Dialogfeld geöffnet. Das kann Timeouts bei anderen geplanten Tasks verursachen.
  - **Nach Timeout schließen:** Bei einem Scan oder Reparaturauftrag, der keinen Neustart vorschreibt, klicken Sie auf diese Option, wenn das Anzeige-Dialogfeld des Scanners nach Abschluss der von Ihnen angegebenen Zeitspanne geschlossen werden soll.
- **CPU-Auslastung beim Scannen:** Gibt Ihnen die Möglichkeit, die Nutzung der CPU durch den Sicherheitsscanner zu steuern, um so die Gesamtleistung des Systems zu verbessern. Wenn mehrere Prozesse gleichzeitig ablaufen und die CPU-Auslastung auf Geräten maximiert wird, können Sie diese Einstellung für den Sicherheitsscanner reduzieren.
- **Status des geplanten Tasks:** Gibt an, auf welcher Ebene Informationen bezüglich des geplanten Sicherheitsscantasks an das Extra "Geplante Tasks" übermittelt werden.

Informationen zur Seite "Scanoptionen"

- **Scannen für:** Gibt an. nach welchen Inhaltstypen Sie mit diesem Scantask suchen möchten. Sie können entweder eine benutzerdefinierte Gruppe (vorkonfiguriert) oder spezifische Inhaltstypen auswählen. Sie können nur Inhaltstypen auswählen, für die Sie ein LANDesk Security Suite-Inhaltsabonnement besitzen. Beachten Sie auch Folgendes: Der Inhalt der Gruppe "Scannen" im Fenster "Patch und Compliance"entscheidet, nach welchen Sicherheitsdefinitionen gescannt wird. Das heißt, wenn Sie in diesem Dialogfeld Anfälligkeiten und Sicherheitsbedrohungen auswählen, wird nur nach den Anfälligkeiten und Sicherheitsbedrohungen gescannt, die aktuell in ihren jeweiligen "Scannen"-Gruppen enthalten sind.
- **Alle erkannten Elemente sofort reparieren:** Zeigt an, dass jedes durch diesen speziellen Gruppenscan erkannte Sicherheitsrisiko automatisch repariert wird.
- **Automatisches Korrigieren aktivieren:** Gibt an, dass der Sicherheitsscanner für alle Anfälligkeiten oder benutzerdefinierten Definitionen, die er auf gescannten Geräten entdeckt, automatisch die vorgeschriebenen Patchdateien bereitstellt und installiert. Diese Option gilt nur für Sicherheitsscan-Tasks. Damit die automatische Korrektur ordnungsgemäß arbeitet, muss "Automatisches Korrigieren" auch für die Patchdatei aktiviert sein.

Informationen zur Seite "Compliance-Einstellungen"

HINWEIS: Compliance-Sicherheitsscans
Beachten Sie, dass die Optionen auf der Seite "Compliance" nur für Compliance-Sicherheitsscans gelten.

- **Scannen:**
  - **Die Compliance-Gruppe häufig scannen:** Führt häufige Sicherheitsscans basierend auf dem Inhalt der Compliance-Gruppe aus. Die Basisversion des häufig auszuführenden Sicherheitsscans wird beim erstmaligen Konfigurieren eines Agenten definiert; Sie können diese Version jedoch mit den Optionen auf dieser Seite überschreiben. Sie können angeben, dass der Compliance-Sicherheitsscan nur ausgeführt wird, wenn ein Benutzer am verwalteten Gerät angemeldet ist.
  - **Nach einer IP-Adressänderung scannen:** Führt einen Compliance-Sicherheitsscan aus, wenn sich die IP-Adresse auf Zielgeräten ändert. Zum Beispiel wenn ein Laptop wieder mit dem Netzwerk verbunden wird und eine andere IP-Adresse erhält als zuvor.
  - **Den häufig auszuführenden Security Scanner in der Agentenkonfiguration deaktivieren:** Gibt an, dass ein häufig auszuführender Sicherheitsscan, der über die Agentenkonfiguration des Geräts eingerichtet wurde, deaktiviert wird und die hier definierten Einstellungen für den häufig auszuführenden Scan stattdessen für einen Compliance-Sicherheitsscan verwendet werden.
- **Aktionen:**
  - **Automatisches Korrigieren aktivieren:** Gibt an, dass der Security Scanner für alle Anfälligkeitsdefinitionen, die er auf gescannten Geräten entdeckt, automatisch die vorgeschriebenen Patchdateien bereitstellt und installiert. Diese Option gilt nur für Sicherheits- und Compliance-Scantasks. Damit die automatische Korrektur ordnungsgemäß arbeitet, muss "Automatisches Korrigieren" auch aktiviert sein.
  - **Alle erkannten Elemente sofort reparieren:** Alle erkannten Anfälligkeit werden repariert, selbst wenn für die ihnen zugeordneten Patches die Option "Automatisches Korrigieren" nicht aktiviert ist.
  - **LANDesk 802.1X-unterstütztes Scannen erzwingen:** Stellt sicher, dass 802.1X-fähige Geräte, die mit diesen Einstellungen auf Sicherheits-Compliance gescannt werden, entweder Zugriff erhalten oder unter Quarantäne gestellt werden, je nachdem, ob sie mit den benutzerdefinierten Sicherheitsrichtlinien übereinstimmen oder nicht.

- **Wenn ein Virus nicht entfernt oder nicht unter Quarantäne gestellt werden kann (nur LANDesk Antivirus):** Die beiden folgenden Optionen beziehen sich nur auf LANDesk Antivirus. Sie bieten Ihnen die Möglichkeit, einen Antivirus-Scan-Auslöser einzurichten oder einen vollständigen Sicherheitsscan zu initiieren, der mit diesen Einstellungen konfigurierte Zielgeräte auf Konformität mit Ihrer aktuellen Sicherheitsrichtlinie überprüft. Mit anderen Worten: ob das Gerät fehlerfrei oder fehlerhaft ist. Sie können eine oder beide der unten beschriebenen Optionen auswählen. Die in diesen Optionen beschriebene Aktion wird immer dann in die Wege geleitet, wenn auf dem Gerät ein Virus erkannt wird und dieser weder entfernt noch unter Quarantäne gestellt werden kann. (**HINWEIS:** Als Bedingung für die Durchführung dieses Scantyps müssen Sie zunächst die vordefinierte AV-110-Virenschutzdefinition der Gruppe "Compliance" hinzufügen. Sie sollten darüber hinaus auch alle anderen Definitionen, die Sie zum Definieren Ihrer Sicherheitsrichtlinie verwenden möchten, der Gruppe "Compliance" hinzufügen.)
    - **Geräte sofort auf Konformität scannen:** Wenn ein Virus erkannt wird und weder entfernt noch unter Quarantäne gestellt werden kann, wird sofort ein Compliance-Sicherheitsscan initiiert (vom Sicherheitsscanner, nicht vom Antivirusscanner).
    - **NAC-Prüfung durchführen, um zu ermitteln, ob das Gerät Fehler aufweist:** Wenn ein Virus erkannt wird, der weder entfernt noch unter Quarantäne gestellt werden kann, führt LANDesk NAC sofort eine Netzwerkzugriffssteuerungsprüfung durch.

Informationen zur Seite "Reparaturoptionen"

- **Vor der Reparatur, Installation oder Deinstallation eines Patchs:** Wählen Sie, ob die Reparatur sofort beginnen soll oder ob auf dem Endbenutzergerät eine Aufforderung mit Nachrichten- und Interaktionssteuerelementen (wie in den nachstehenden Optionen konfiguriert) angezeigt werden soll oder ob Sie mit der Durchführung der Reparatur warten möchten, bis das Gerät gesperrt und der Benutzer abgemeldet ist.
- **Meldung:** Geben Sie in dieses Feld eine Meldung ein, die im Anzeige-Dialogfeld des Sicherheitsscanners auf dem Gerät des Endbenutzers angezeigt wird, WENN ein Sicherheitsscantask eine der angegebenen Definitionen auf dem gescannten Gerät erkennt. Sie können diese Meldung an den von Ihnen ausgeführten Sicherheitsscan anpassen.
- **Wenn keine Benutzerantwort:**
    - **Mit dem Reparieren, Installieren oder Deinstallieren warten, bis der Benutzer geantwortet hat:** Bei einer Benutzerabfrage zu einem Patchdatei-Vorgang, die unbeantwortet bleibt, klicken Sie auf diese Option, wenn Sie den Scanner anweisen möchten, weiterhin auf unbestimmte Zeit zu warten.
    - **Nach Timeout automatisch:** Für eine Benutzerabfrage zu einem Patchdatei-Vorgang, die nicht beantwortet wird, klicken Sie auf diese Option, wenn Sie den Scanner anweisen möchten, nach der von Ihnen angegebenen Zeitspanne automatisch fortzufahren und den Patchdatei-Vorgang auszuführen oder den Scanner zu schließen, ohne den Vorgang auszuführen.
- **Reparatur auch in folgenden Situationen starten:**
    - **Der Benutzer zeigt gerade eine Präsentation:** Gibt an, dass die Reparatur unabhängig davon beginnt, ob die Anwendung Microsoft Office PowerPoint auf dem Gerät ausgeführt wird.
    - **Der Neustart steht bereits an:** Gibt an, dass die Reparatur gestartet wird, ohne die Neustartoperation abzuwarten.
- **Maximale Bandbreite bei Download von Quelle:** Gibt den Bandbreitenprozentsatz an, der für den Download der Patchdatei auf gescannte Geräte aus dem Patchrepository verwendet werden soll. Sie können mit diesen Einstellungen die Netzwerkbelastung bei großen Patchdatei-Bereitstellungen gleichmäßiger verteilen.

- **Maximale Bandbreite bei Download von Peer:** Gibt den Bandbreitenprozentsatz an, der für den Download der Patchdatei von einem Peergerät verwendet werden soll. Sie können mit diesen Einstellungen die Netzwerkbelastung bei großen Patchdatei-Bereitstellungen gleichmäßiger verteilen.

Informationen zur Seite "MSI-Informationen"

Diese Seite verwenden Sie, wenn eine Patchdatei auf ihre ursprüngliche Produkt-Installationsressource zugreifen muss, um erforderliche Zusatzdateien zu installieren. Diese Informationen werden u.U. benötigt, wenn Sie versuchen, ein Patch für Microsoft Office oder eine andere Produkt-Suite anzuwenden.

- **Speicherort des Originalpakets:** Geben Sie den UNC-Pfad zum Produktabbild ein.
- **Zu verwendende Anmeldeinformationen, wenn auf den Speicherort des Originalpakets verwiesen wird:** Geben Sie einen gültigen Namen und ein gültiges Kennwort für die Authentifizierung bei der oben angegebenen Netzwerkfreigabe ein.
- **/overwriteoem-Befehlszeilenoption ignorieren:** Gibt an, dass der Befehl zum Überschreiben OEM-spezifischer Instruktionen ignoriert wird. Das heißt mit anderen Worten, dass die OEM-Instruktionen ausgeführt werden.
- **Als Information ausführen: Anmeldeinformationen zum Ausführen von Patches:** Geben Sie einen gültigen Benutzernamen und ein Kennwort ein, um den angemeldeten Benutzer zum Ausführen von Patches zu identifizieren.

Informationen zur Seite "Neustartoptionen"

- **Bei der Entscheidung, ob ein Neustart durchgeführt werden soll:** Geben Sie an, wie sich der Sicherheitsscanner verhalten soll, wenn ein Scan- oder Reparaturtask aus irgendeinem Grund versucht, ein Gerät neu zu starten. Sie können "Nie neu starten", "Nur bei Bedarf neu starten" oder "Immer neu starten" auswählen.
- **Während des Neustarts:**
    - **Benutzerabfrage vor dem Neustart:** Für den Fall, dass ein Neustart erfolgt, klicken Sie auf diese Option, wenn Sie veranlassen möchten, dass der Sicherheitsscanner eine Benutzerabfrage einblendet. Wenn Sie diese Option auswählen, können Sie zusätzlich die nachstehend beschriebenen Neustartoptionen konfigurieren:
    - **Sofern niemand angemeldet ist, sofort ohne Abfrage oder Verzögerung neu starten:** Stellt sicher, dass der Neustart automatisch erfolgt, für den Fall, dass derzeit niemand auf dem Gerät angemeldet ist.
    - **Benutzer darf Neustart verzögern:** Blendet in der Neustartabfrage auf dem Gerät des Benutzer eine Verzögerungsschaltfläche ein. Geben Sie den Verzögerungszeitraum an und legen Sie fest, wie oft der Benutzer den Neustart verzögern kann. Die Verzögerungszeit beginnt beim nächsten Local Scheduler-Poll. (Beachten Sie, dass die Verzögerungszeit bedingt durch den Local Scheduler-Einsatz 10 Minuten beträgt.)
    - **Benutzer darf Neustart abbrechen:** Blendet in der Neustartabfrage auf dem Gerät des Benutzers eine Schaltfläche zum Abbrechen ein.
    - **Neustartmeldung:** Geben Sie in dieses Feld eine Meldung ein, die im Anzeige-Dialogfeld des Sicherheitsscanners auf dem Gerät des Endbenutzers angezeigt wird, WENN ein Sicherheitsscantask vor dem Versuch, ein Gerät neu zu starten, eine Abfrage an den Endbenutzer richtet.
    - **Erst nach Erhalt der Benutzerantwort neu starten:** Für eine Neustart-Benutzerabfrage, die nicht beantwortet wird, klicken Sie auf diese Option, wenn Sie den Scanner anweisen möchten, weiterhin auf unbestimmte Zeit zu warten. Wenn es keine Antwort gibt, bleibt die Benutzerabfrage geöffnet.

- **Nach Timeout automatisch:** Für einer Benutzerabfrage zu einem Patchdatei-Vorgang, die unbeantwortet bleibt, klicken Sie auf diese Option, wenn Sie den Scanner anweisen möchten, nach der von Ihnen angegebenen Zeitspanne, automatisch fortzufahren und den Patchdatei-Vorgang auszuführen, oder den Scanner zu schließen, ohne den Vorgang auszuführen.

Informationen zur Seite "Netzwerkeinstellungen"

Diese Seite verwenden Sie, um einen alternativen Coreserver zu benennen, der für Sicherheitsscans und Reparaturen eingesetzt werden kann, wenn der Haupt-Coreserver nicht verfügbar ist.

- **Mit alternativem Coreserver kommunizieren:** Ermöglicht die Kommunikation mit einem alternativen Server.
- **Servername:** Geben Sie hier den Namen eines gültigen, lizenzierten LANDesk Coreservers ein.

WICHTIG: Die Syntax für das Servernamensfeld sollte wie folgt sein: <Servername>:<Anschlussnummer> wobei Anschlussnummer der sichere Anschluss 443 für die SSL-Übertragung ist. Wenn Sie nur einen Servernamen eingeben und Anschluss 443 nicht angeben, wird der Standard-HTTP-Anschluss Anschluss 80 verwendet.

Informationen zur Seite "Pilotkonfiguration"

Diese Seite verwenden Sie zum Erstellen und Konfigurieren einer Pilotgruppe zum Testen der Sicherheitsdefinitionen, bevor Sie die Bereitstellung auf Ihrem gesamten Netzwerk durchführen.

- **Definitionen in folgenden Gruppen regelmäßig scannen und reparieren:** Aktiviert die Pilotsicherheitsfunktionen. Sobald Sie diese Option aktiviert haben, müssen Sie eine benutzerdefinierte Gruppe aus der Dropdownliste auswählen.
- **Einstellungen ändern:** Öffnet das Dialogfeld "Planen". Hier können Sie die Parameter für Sicherheitsscans definieren. Klicken Sie auf die Schaltfläche **Hilfe**, wenn Sie Genaueres wissen möchten.

Informationen zum Dialogfeld "Periodisches Scannen und Reparieren planen (Pilotscan)"

Dieses Dialogfeld wird von mehreren LANDesk Verwaltungstasks gemeinsam genutzt. Details über die Optionen in diesem Dialogfeld finden Sie in Informationen zum Dialogfeld "Planen".

Informationen zur Seite "Spyware-Scannen"

Diese Seite verwenden Sie, um die Spyware-Einstellungen in der Agentenkonfiguration eines Geräts zu ersetzen (oder zu überschreiben).

Die Spyware-Erkennung in Echtzeit überwacht Geräte auf neu gestartete Prozesse, die versuchen, die lokale Registrierung zu manipulieren. Wenn Spyware erkannt wird, fordert der Sicherheitsscanner des Geräts den Endanwender auf, die Spyware zu entfernen.

Diese Seite enthält folgende Optionen:

- **Einstellungen aus der Agentenkonfiguration überschreiben:** Ersetzt vorhandene Spyware-Einstellungen auf Geräten, die ursprünglich über eine Agentenkonfiguration konfiguriert wurden. Verwenden Sie die nachstehend beschriebenen Optionen, um die neuen Spyware-Einstellungen festzulegen, die Sie für Zielgeräte bereitstellen möchten.

- **Einstellungen:**
  - **Echtzeit-Spywareblockierung aktivieren:** Aktiviert Spyware-Überwachung und Blockierung in Echtzeit auf Geräten, die über diese Agentenkonfiguration verfügen.

    HINWEIS: Damit das Echtzeit-Spyware-Scanning und die Spyware-Erkennung funktioniert, müssen Sie die automatische Korrekturfunktion manuell aktivieren, um die heruntergeladenen Spyware-Definitionen im Sicherheitsscan einzuschließen. Die automatische Reparaturfunktion ist für heruntergeladene Spyware-Definitionen standardmäßig nicht eingeschaltet.

  - **Benutzer benachrichtigen, wenn Spyware blockiert wurde:** Zeigt eine Meldung an, die den Endanwender informiert, dass ein Spyware-Programm erkannt und repariert wurde.
  - **Wenn eine Anwendung nicht als Spyware erkannt wird, die Genehmigung des Benutzers für die Installation anfordern:** Selbst wenn der erkannte Prozess nicht als Spyware eingestuft wird (gemäß der aktuellen Liste der Spyware-Definitionen für dieses Gerät), wird der Benutzer dennoch zur Bestätigung aufgefordert, bevor die Software auf dem Computer installiert wird.

Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen konfigurieren"

Dieses Dialogfeld verwenden Sie, um Ihre Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen zu verwalten. Nachdem Sie Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen konfiguriert haben, können Sie diese auf einen Einstellungsänderungstask anwenden und den Task auf Zielgeräten bereitstellen, um die Standardeinstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen zu ändern (oder zu entfernen).

Durch die Außerkraftsetzung benutzerdefinierter Variablen können Sie Ausnahmen für benutzerdefinierte Variablenwerte konfigurieren. Mit anderen Worten können Sie mithilfe der Einstellungen zur Außerkraftsetzung benutzerdefinierter Variablen eine bestimmte Bedingung für eine benutzerdefinierte Variable ignorieren oder umgehen, sodass das gescannte Gerät nicht als anfällig erkannt wird.

Dieses Dialogfeld enthält folgende Optionen:

- **Neu:** Öffnet das Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen", in dem Sie Optionen konfigurieren können.
- **Bearbeiten:** Öffnet das Dialogfeld "Einstellungen", in dem Sie die ausgewählten Einstellungen zur Außerkraftsetzung einer benutzerdefinierten Variablen ändern können.
- **Kopieren:** Öffnet eine Kopie der ausgewählten Einstellungen als Vorlage, die von Ihnen dann bearbeitet und umbenannt werden können.
- **Löschen:** Entfernt die ausgewählten Einstellungen aus der Datenbank.

  HINWEIS: Die ausgewählten Einstellungen sind zur Zeit möglicherweise mit Tasks oder verwalteten Geräten verknüpft. Wenn Sie diese Einstellungen löschen, verfügen Geräte mit diesen Einstellungen weiterhin über diese Einstellungen und verwenden diese auch nach wie vor, bis ein neuer Task vom Typ "Einstellungen ändern" bereitgestellt wird; geplante Tasks, die über diese Einstellungen verfügen, werden weiterhin auf Zielgeräten ausgeführt, genauso wie Local Scheduler-Tasks, die über diese Einstellungen verfügen. Auch sie werden solange ausgeführt, bis eine neue Konfiguration bereitgestellt wird.

- **Schließen:** Schließt das Dialogfeld, ohne Einstellungen auf den Task anzuwenden.

Informationen zum Dialogfeld "Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen"

Dieses Dialogfeld verwenden Sie, um Ausnahmen für Einstellungen für eine benutzerdefinierte Variable zu erstellen. Einige Definitionen für Sicherheitsbedrohungen der Systemkonfiguration verfügen beispielsweise über Einstellungen, die Sie ändern können, bevor Sie sie in einem Sicherheitsscan einschließen. Normalerweise verfügen Virenschutzdefinitionen auch über Einstellungen für benutzerdefinierte Variablen.

Mit benutzerdefinierten Variablen können Sie das Scannen auf Sicherheitsbedrohungen optimieren, indem Sie die Werte einer oder mehrerer Einstellungen so ändern, dass der Scanner nach von Ihnen definierten Bedingungen sucht und das Gerät nur dann als anfällig erkennt, wenn diese spezielle Bedingung erfüllt ist (d. h. der von Ihnen angegebene Wert vorgefunden wird). Benutzerdefinierte Variablen sind globale Einstellungen. Das heißt, dass beim Scannen nach einer Sicherheitsdefinition, die eine benutzerdefinierte Variable enthält, diese immer als anfällig ausgewiesen wird, sofern die Bedingung dieser benutzerdefinierten Variable erfüllt wird.

WICHTIG: Das Recht "Benutzerdefinierte Variablen bearbeiten" ist erforderlich
Um Einstellungen für benutzerdefinierte Variablen bearbeiten und Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen konfigurieren zu können, muss der LANDesk Benutzer über das rollenbasierte Administrationsrecht "Benutzerdefinierte Variablen bearbeiten" verfügen. Rechte werden mit dem Extra **Benutzer** konfiguriert.

Informationen zur den Einstellungen zur Außerkraftsetzung von benutzerdefinierten Variablen werden in der Inventaransicht des Geräts angezeigt.

Informationen zum Dialogfeld "Definitionsgruppeneinstellungen"

Dieses Dialogfeld verwenden Sie, um Einstellungen zu erstellen, zu bearbeiten und auszuwählen, die steuern, wie und wo Sicherheitsdefinitionen heruntergeladen werden, aufgrund ihres Typs und/oder Schweregrads.

Dieses Dialogfeld enthält folgende Optionen:

- **Definitionstyp- und Schweregradfilter:** Führt die Definitionsgruppeneinstellungen auf.
- **Typ:** Zeigt den Definitionstyp der ausgewählten Gruppeneinstellungen.
- **Schweregrad:** Zeigt den Definitionsschweregrad der ausgewählten Gruppeneinstellungen.
- **Vergleich:**
- **Status:** Zeigt den Status ("Nicht scannen", "Scannen" und "Nicht zugewiesen") für Definitionen, die den Gruppeneinstellungen entsprechen, wenn sie heruntergeladen werden. Der Status entspricht den Gruppenknoten in der Strukturansicht. Der Standardzustand ist "Nicht zugewiesen".
- **Gruppe(n):** Zeigt die Gruppe oder Gruppen, deren Sicherheitsdefinitionen mit dem o.g. Typ und Schweregrad übereinstimmen. Sie können so viele benutzerdefinierte Gruppen hinzufügen und löschen, wie Sie möchten.
- **Automatisches Korrigieren:** Wenn Sie angegeben haben, dass die heruntergeladenen Sicherheitsdefinitionen auf "Scannen" eingestellt sind (in die Gruppe "Scannen" aufgenommen), wählen Sie diese Option, sofern Sie wünschen, dass für Anfälligkeiten "Automatisches Korrigieren" aktiviert werden soll.
- **Ersetztes deaktivieren:**

Informationen zum Dialogfeld "Definitionsfiltereigenschaften"

Dieses Dialogfeld verwenden Sie zur Definition der Definitionsgruppeneinstellungen. Diese Einstellungen regeln, wie und wo Sicherheitsdefinitionen heruntergeladen werden, je nach ihrem Typ und/oder Schweregrad.

Dieses Dialogfeld enthält folgende Optionen:

- **Filter:** Definiert, welcher Sicherheitsinhalt (Definitionen) in die nachstehend ausgewählten Gruppen aufgenommen werden.
  - **Definitionstyp:** Wählen Sie den Definitionstyp aus, den Sie downloaden möchten, sowie den gewünschten Status und Speicherort.
  - **Schweregrad:** Wählen Sie den Schweregrad des angegebenen Definitionstyps aus. Wenn zwar der Typ passt, aber der Schweregrad nicht, wird die Definition nicht von diesen Einstellungen gefiltert.
- **Aktion:** Definiert, was Sie mit den heruntergeladenen Definitionen anfangen möchten und wo sie gespeichert werden sollen.
  - **Status festlegen:** Wählen Sie den Status des angegebenen Definitionstyps aus. Zu den Optionen gehören: "Nicht scannen", "Scannen" und "Nicht zugewiesen".
  - **Automatisches Korrigieren einstellen:** Wählen Sie "Automatisches Korrigieren" aus, wenn der Status "Scannen" ist und Sie möchten, dass das Sicherheitsrisiko automatisch bei der Erkennung korrigiert wird.
  - **Definition in benutzerdefinierter/n Gruppe(n) einfügen:** Wählen Sie mit den Schaltflächen "Hinzufügen" oder "Löschen" mindestens eine Gruppe aus. Sie können jede der von Ihnen erstellten benutzerdefinierten Gruppen auswählen, die Alarmgruppe, die Compliant-Gruppe und einige der verfügbaren Sicherheitsbranchengruppen.

Informationen zum Dialogfeld "Alarmeinstellungen"

Dieses Dialogfeld verwenden Sie zum Konfigurieren von Sicherheitsalarmen (Anfälligkeits- und Antivirus-Alarme etc.).

Das Dialogfeld "Alarmeinstellungen" umfasst die folgenden Seiten:

Seite "Definitionen"

Diese Seite verwenden Sie zum Konfigurieren der Sicherheitsalarmierung. Wenn Sie der Gruppe "Alarm" Sicherheitsdefinitionen hinzugefügt haben, werden Sie von "Patch und Compliance" gewarnt, wenn eine dieser Definitionen auf irgendeinem gescannten Gerät entdeckt wird.

- **Mindestalarmintervall:** Gibt den kürzesten Zeitabstand an (in Minuten oder Stunden), in dem Alarmmeldungen für erkannte Viren gesandt werden. Sie können diese Einstellungen verwenden, falls Sie nicht zu oft gewarnt werden möchten. Stellen Sie den Wert auf Null ein, falls Sie immer sofort in Echtzeit gewarnt werden möchten.
- **Zur Alarmgruppe hinzufügen:** Gibt an, welche Anfälligkeiten (nach Schweregrad) während eines Inhalt-Downloads automatisch der Alarmgruppe hinzugefügt werden. Jede Definition, die in die Alarmgruppe platziert wird, wird standardmäßig auch automatisch in die Gruppe "Scannen" platziert (um diese Definitionen in einen Sicherheitsscan-Task einzuschließen).

Seite "Antivirus"

Diese Seite verwenden Sie zum Konfigurieren der Antivirusalarmierung.

- **Mindestalarmintervall:** Gibt den kürzesten Zeitabstand an (in Minuten oder Stunden), in dem Alarmmeldungen für erkannte Viren gesandt werden.. Sie können diese Einstellungen verwenden, falls Sie nicht zu oft gewarnt werden möchten. Stellen Sie den Wert auf Null ein, falls Sie immer sofort in Echtzeit gewarnt werden möchten.
- **Alarm auf:** Gibt an, welche Antivirus-Ereignisse Alarme generieren.

Informationen zum Dialogfeld "Core-Einstellungen"

Dieses Dialogfeld verwenden Sie, um die automatische Weiterleitung der jüngsten Sicherheitsscanergebnisse an einen Rollup-Coreserver in Ihrem Netzwerk zu aktivieren und zu konfigurieren. Durch die Weiterleitung von Sicherheitsscandaten erhalten Sie die Möglichkeit, den Anfälligkeitsstatus für Ihre sämtlichen verwalteten Geräte in einem großen verteilten Unternehmensnetzwerk in Echtzeit anzuzeigen, ohne die Daten direkt vom primären Coreserver abrufen zu müssen.

Bei jedem Ausführen des Sicherheitsscanners wird eine Scanergebnisdatei in einen Ordner namens "VulscanResults" auf dem Coreserver geschrieben. Ferner wird der LANDesk Security Suite-Webdienst benachrichtigt, der die Datei dann zur Coredatenbank hinzufügt. Wenn die Rollup-Core-Einstellungen aktiviert sind und ein gültiger Rollup-Core erkannt wird, liest der Rollup-Core die Scanergebnisdatei in seine eigene Datenbank, sodass der Zugriff auf kritische Anfälligkeitsdaten beschleunigt wird.

Dieses Dialogfeld enthält folgende Optionen:

- **Scanergebnisse:**
  - **Scanergebnisse nach der Verarbeitung im Ordner "vulscanresults" speichern:** Speichert die Ergebnisdateien des Sicherheitsscans im vulscan-Standardordner.
  - **Dateien dekomprimieren (falls erforderlich):** Aktiviert die automatische Dekomprimierung der Scanergebnisdateien, falls diese in komprimierter Form vorliegen.
- **Anzahl der Wiederholversuche für "Automatisches Korrigieren":**
  - **Automatisches Korrigieren nach *n* Versuchen aufgeben:** Gibt an, wie oft der Coreserver das Reparieren mit der Funktion "Automatisches Korrigieren" versuchen wird, bevor es zum Timeout kommt.
  - **Automatisches Korrigieren immer wieder versuchen:** Zeigt an, dass der Coreserver die Reparatur mit "Automatisches Korrigieren" so lange versuchen wird, bis die Funktion erfolgreich ausgeführt wurde oder bis Sie den Prozess stoppen.

- **Rollup-Core:**
  - **Scanergebnisse sofort an Rollup-Core senden:** Ermöglicht die sofortige Weiterleitung von Sicherheitsscanergebnissen an den angegebenen Coreserver mithilfe des oben beschriebenen Verfahrens.
  - **Standard-Rollup-URL benutzen:** Aktivieren Sie dieses Kontrollkästchen, wenn Sie veranlassen möchten, dass beim Senden der Scanergebnisdatei vom Coreserver an den Rollup-Core die Standard-URL verwendet werden soll. Geben Sie den Namen des Coreservers ein und aktivieren Sie anschließend dieses Kontrollkästchen, damit das Script und die Webadresse automatisch in das **Rollup-URL**-Feld eingefügt werden.
  - **Name des Rollup-Core:** Identifiziert den Rollup-Core, an den die neuesten Sicherheitsscanergebnisse von der Coredatenbank gesendet werden sollen.
  - **Rollup-URL:** Gibt die Webadresse des Rollup-Cores an, an den die Sicherheitsscanergebnisse weitergeleitet werden, sowie den Zielordner für die Scanergebnisdatei auf dem Rollup-Core. Die Rollup-URL kann entweder automatisch eingefügt werden, indem das Kontrollkästchen **Standard-Rollup-URL benutzen** aktiviert wird, oder Sie können das Feld manuell bearbeiten, indem Sie das Kontrollkästchen deaktivieren und eine URL Ihrer Wahl eingeben.

Informationen zum Dialogfeld "Berechtigungen"

Dieses Dialogfeld verwenden Sie, um die effektiven Berechtigungen anzuzeigen, die der derzeit angemeldete Administrator in Bezug auf das Extra "Patch und Compliance" besitzt. Diese Einstellungen für Berechtigungen werden mit dem Extra "Benutzerverwaltung" konfiguriert. Ein LANDesk Administrator kann außerdem die rollenbasierten Berechtigungen ändern, die zum Bearbeiten und Importieren von benutzerdefinierten Anfälligkeitsdefinitionen erforderlich sind.

WICHTIG: Die rollenbasierte Berechtigung kann ausschließlich von einem LANDesk Administrator geändert werden.

Dieses Dialogfeld enthält folgende Optionen:

- **Benutzer:**
  - **Ansicht:** Zeigt an, dass der Benutzer Patchsicherheitsinhalte anzeigen kann.
  - **Bearbeiten:** Zeigt an, dass der Benutzer Patchsicherheitsinhalte bearbeiten kann.
  - **Bereitstellen:** Zeigt an, dass der Benutzer Patchsicherheitsinhalte bereitstellen kann.
  - **Öffentlich bearbeiten:** Zeigt an, dass der Benutzer Inhalte für benutzerdefinierte Anfälligkeiten bearbeiten kann.
- **Bedeutung der rollenbasierten Berechtigungen:**
  - **Berechtigung "Öffentlich bearbeiten" zum Bearbeiten von benutzerdefinierten Definitionen erforderlich:** Gibt an, dass ein Benutzer nur dann benutzerdefinierte Anfälligkeitsdefinitionen bearbeiten kann, wenn er die Berechtigung "Öffentlich bearbeiten" besitzt.
  - **Berechtigung "Öffentlich bearbeiten" zum Importieren von Definitionen erforderlich:** Gibt an, dass ein Benutzer nur dann Sicherheitsdefinitionen importieren kann, wenn er die Berechtigung "Öffentlich bearbeiten" besitzt.

Hilfe zur Patch und Compliance-Symbolleiste

Informationen zum Dialogfeld "Patch- und Compliancedefinitionen löschen"

Verwenden Sie dieses Dialogfeld zum Entfernen von Definitionen (und den mit ihr verknüpften Erkennungsregeln) aus der Coredatenbank.

WICHTIG: Erfordert das LANDesk Administrator-Recht
Ein Benutzer muss das LANDesk Administrator-Recht besitzen, um diesen Task ausführen zu können.

Es empfiehlt sich, Definitionen zu entfernen, wenn Sie veraltet sind, nicht wie vorgeschrieben funktionieren oder das von ihnen ausgehende Sicherheitsrisiko komplett beseitigt wurde.

Dieses Dialogfeld enthält folgende Optionen:

- **Plattformen:** Gibt die Plattformen an, deren Definitionen Sie aus der Datenbank entfernen möchten. Falls eine Definition mit mehreren Plattformen verknüpft ist, müssen Sie alle mit der Definition verknüpften Plattformen auswählen, damit die Definition inklusive Erkennungsregel entfernt wird.
- **Sprachen:** Gibt an, von welchen Sprachversionen der ausgewählten Plattformen Sie die Definitionen aus der Datenbank löschen möchten. Wenn Sie eine Windows- oder Macintosh-Plattform ausgewählt haben, sollten Sie die Sprachen angeben, deren Definitionsinformationen Sie entfernen möchten. Wenn Sie eine UNIX- oder Linux-Plattform ausgewählt haben, müssen Sie die Option "Sprache neutral" auswählen, damit die sprachübergreifenden Definitionsinformationen dieser Plattformen entfernt werden.
- **Typen:** Gibt die Inhaltstypen an, deren Definitionen Sie entfernen möchten.
- **Entfernen:** Entfernt Definitions- und Erkennungsregelinformationen für die Typen, die Sie ausgewählt haben und die zu den angegebenen Plattformen und Sprachen gehören. Diese Informationen können nur durch erneuten Download des Inhalts wiederhergestellt werden.
- **Schließen:** Schließt das Dialogfeld, ohne Änderungen zu speichern und Definitionsinformationen zu entfernen.

Informationen über die Informationsansicht zum Sicherheitsscan

Dieses Dialogfeld verwenden Sie, um detaillierte Informationen zum Status der Patchbereitstellung und damit verbundenen Aktivitäten für verwaltete Geräte in Ihrem Netzwerk anzuzeigen.

Folgende Scanergebnisse können Sie anzeigen:

- Computer, die in jüngster Zeit nicht Bericht erstattet haben
- Computer ohne Ergebnisse
- Computers, die Patches erfordern. Geordnet nach Schweregrad.

Informationen zum Dialogfeld "Grenzwerteinstellungen"

Dieses Dialogfeld verwenden Sie, um Zeiträume für Antivirus-Scan-(Patchbereitstellungs-)Ergebnisse zu definieren, die im Dialogfeld **Sicherheitsscaninformationen** angezeigt werden.

- **Grenzwert für "Nicht kürzlich gescannt":** Gibt an, wie viele Tage maximal nach Geräten gesucht werden soll, die nicht auf Patchbereitstellung gescannt wurden.

Informationen zum Dialogfeld "Sicherheits- und Patchinformationen"

Dieses Dialogfeld verwenden Sie, um detaillierte Sicherheitsinformationen für ausgewählte Geräte anzuzeigen. Sie können die Scanergebnisse eine Geräts, erkannte Sicherheitsdefinitionen, fehlende und installierte Patches (oder Softwareupdates) sowie Reparaturprotokolle anzeigen.

Verwenden Sie die Schaltfläche **Löschen**, um alle Scaninformationen aus der Datenbank zu entfernen, die sich auf die ausgewählten Geräte beziehen.

Sie können in dieser Ansicht mit der rechten Maustaste auf eine Anfälligkeit (oder einen Sicherheitsinhalt) klicken und sofort einen Reparaturtask erstellen oder die Funktion "Automatisches Korrigieren" für die relevanten Sicherheitsinhalte aktivieren oder deaktivieren.

Welche Informationen angezeigt werden, ist vom ausgewählten Sicherheitsinhalt abhängig.

Die Gruppennamen- und Informationsfelder auf dieser Seite sind dynamisch, je nachdem, welchen Sicherheitsinhalts-Typ Sie in der Dropdownliste **Typ** auswählen. Wenn Sie Anfälligkeiten wählen, werden beispielsweise folgende Felder angezeigt:

- **Fehlende Patches (Anfälligkeiten erkannt):** Listet alle Anfälligkeiten auf, die vom letzten Scan auf dem Gerät erkannt wurden.
- **Installierte Patches:** Listet alle Patches auf, die auf dem Gerät installiert sind.
- **Reparaturverlauf:** Zeigt Informationen zu den auf diesem Gerät versuchten Reparaturtasks an. Diese Informationen sind ein nützliches Hilfsmittel bei der Fehlerbehebung. Um diese Daten zu löschen, klicken Sie auf **Reparaturverlauf löschen**, geben die Geräte und die Zeitraumoptionen an und klicken auf **Löschen**.
- **Anfälligkeitsinformationen:**
  - **Titel:** Zeigt den Titel der ausgewählten Anfälligkeit an.
  - **Erkannt:** Gibt an, ob die ausgewählte Anfälligkeit erkannt wurde.
  - **Zuerst erkannt:** Zeigt das Datum und die Uhrzeit an, zu der die Anfälligkeit zum ersten Mal auf dem Gerät erkannt wurde. Diese Informationen können nützlich sein, wenn Sie mehrere Scans ausgeführt haben.
  - **Grund:** Beschreibt den Grund für die Erkennung der ausgewählten Anfälligkeit. Diese Information kann hilfreich sein bei der Entscheidung, ob die Anfälligkeit ein so ernstes Sicherheitsrisiko darstellt, dass sofort Abhilfe geschaffen werden muss.
  - **Erwartet:** Zeigt die Versionsnummer der Datei oder des Registrierungsschlüssels an, nach dem der Anfälligkeitsscanner sucht. Falls die Versionsnummer der Datei oder des Registrierungsschlüssels auf dem gescannten Gerät dieser Nummer entspricht, dann ist keine Anfälligkeit gegeben.
  - **Gefunden:** Zeigt die Versionsnummer der Datei oder des Registrierungsschlüssels an, die auf dem gescannten Gerät festgestellt wurde. Falls sich diese Nummer von der oben erwarteten Nummer unterscheidet, ist eine Anfälligkeit gegeben.
- **Patchinformationen:**
  - **Patch erforderlich:** Zeigt den Dateinamen des ausführbaren Patches an, der zur Behebung der ausgewählten Anfälligkeit erforderlich ist.
  - **Patch installiert:** Gibt an, ob die Patchdatei installiert wurde.
  - **Letztes Aktionsdatum:** Zeigt Datum und Uhrzeit der Patchinstallation auf dem Gerät an.
  - **Aktion:** Gibt an, ob die letzte Aktion eine Installation oder Deinstallation war.

- **Details:** Gibt an, ob die Bereitstellung/Installation erfolgreich ausgeführt wurde. Falls die Installation fehlschlug, müssen Sie diese Statusinformationen löschen, bevor Sie versuchen, das Patch erneut zu installieren.
- **Löschen:** Löscht das aktuelle Patchinstallationsdatum und die Statusinformationen für das ausgewählte Gerät. Diese Informationen müssen gelöscht werden, um einen erneuten Bereitstellungs- und Installationsversuch mit dem Patch durchführen zu können.

Sicherheitskonfigurationen

Agenteneinstellungen – Übersicht

Das neue Extra "Agenteneinstellungen" stellt ein praktisches separates Fenster bereit, in dem Sie Konfigurationen für mehrere LANDesk Security Suite Komponenten und Dienste sowie zugehörige Bereitstellungstasks erstellen und verwalten können.

Agenteneinstellungen steuern, wie Sicherheitsdienste auf verwalteten Geräten ausgeführt werden. Sicherheitsdienste und zugehörige Einstellungen können im Rahmen der anfänglichen Agentenkonfiguration für Ihre verwalteten Geräte bereitgestellt werden, als separate Installation- oder Updatetasks und als Einstellungsänderungstasks.

Mit Agenteneinstellungen können Sie Einstellungen für folgende Sicherheitsdienste erstellen und verwalten:

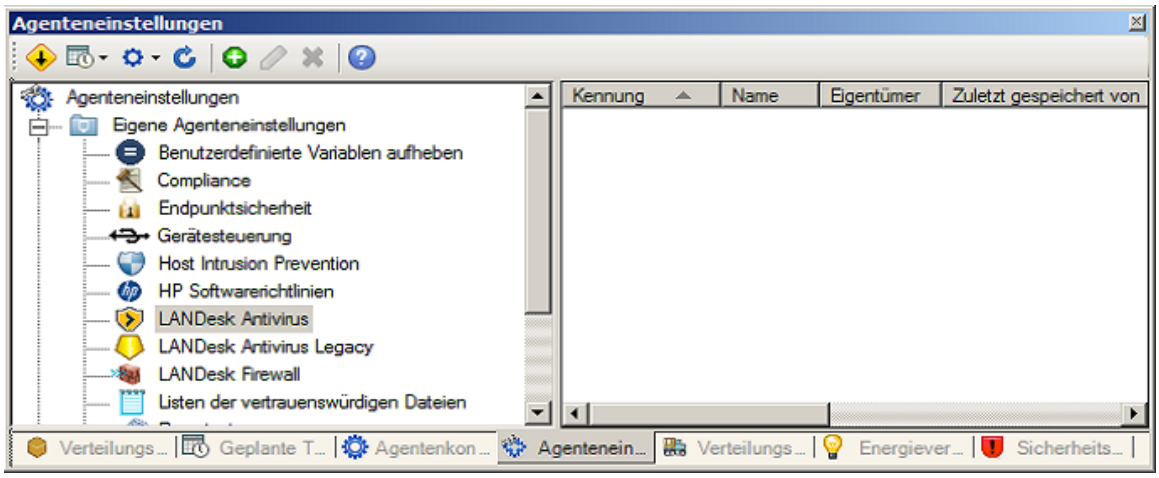
- Compliance
- Benutzerdefinierte Variablen aufheben
- Gerätesteuerung
- Windows-Firewall
- Endpunktsicherheit (HIPS, LANDesk Firewall und Gerätesteuerung)
- Host Intrusion Prevention
- HP Softwarerichtlinien
- LANDesk Antivirus
- LANDesk Antivirus Legacy
- LANDesk Firewall
- Remotesteuerung
- Scannen und Reparieren
- Listen der vertrauenswürdigen Dateien
- Windows-Firewall

Ferner können Sie die in diesem Abschnitt beschriebenen Tasks für Sicherheitskomponenten durchführen.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Agenteneinstellungen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Konfigurieren von Sicherheitseinstellungen und -Tasks

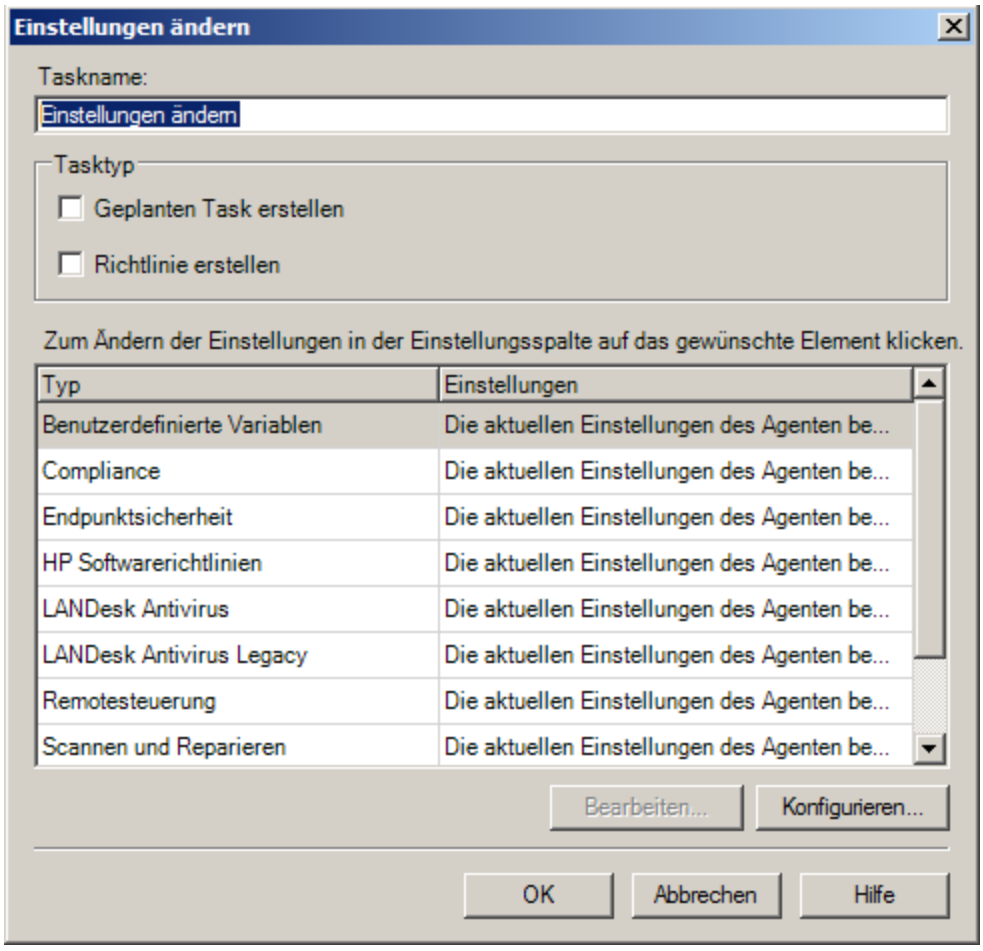
Das Fenster des Extras "Agenteneinstellungen" bietet eine praktische Schnittstelle, über die Sie Einstellungen und Tasks für mehrere Sicherheitskomponenten und -dienste verwalten können.



Erstellen von Einstellungsänderungstasks

Die Sicherheits-Standardeinstellungen der Geräte werden als Teil der ursprünglichen Agentenkonfiguration bereitgestellt. Es kann zu einem späteren Zeitpunkt sinnvoll sein, diese Standardeinstellungen auf bestimmten Geräten zu ändern. Das Extra "Agenteneinstellungen" bietet eine Möglichkeit, diese Änderungen vorzunehmen, ohne erneut eine komplett neue und vollständige Agentenkonfiguration bereitstellen zu müssen.

Verwenden Sie hierfür den Task **Einstellungen ändern** in der Symbolleistenschaltfläche **Task erstellen**.



In das eingeblendete Dialogfeld können Sie einen eindeutigen Namen für den Task eingeben, festlegen, ob es sich um einen geplanten Task oder eine Richtlinie handelt, und entweder eine vorhandene Einstellung als Standard auswählen oder mithilfe der Schaltfläche "Bearbeiten" eine neue Einstellung als Standard für Zielgeräte erstellen.

Hilfe zum Ändern von Einstellungen

Informationen zum Dialogfeld "Einstellungsänderungstask erstellen"

Dieses Dialogfeld verwenden Sie, um einen Task zu erstellen und zu konfigurieren, der die Standardeinstellungen auf Zielgeräten für Komponenten der Endpunktsicherheit ändert.

Mit einem Einstellungsänderungstask lassen sich die Standardeinstellungen eines Geräts (die in die lokale Registrierung des Geräts geschrieben werden) bequem ändern, ohne erneut eine vollständige Agentenkonfiguration bereitstellen zu müssen.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Geben Sie zur Identifizierung des Tasks einen eindeutigen Namen ein.
- **Geplanten Task erstellen:** Fügt den Task dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.

- **Richtlinie erstellen:** Fügt den Task als Richtlinie dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **Typ:** Identifiziert die Sicherheitskomponente.
- **Endpunktsicherheit:** Gibt die Einstellungen für die Endpunktsicherheit an, die diesem spezifischen Einstellungsänderungstask zugeordnet sind. Denken Sie daran, dass die Endpunktsicherheit, obwohl sie als einzelner Agent für Zielgeräte bereitgestellt wird, Dienste für mehrere Sicherheitskomponenten bereitstellt. Hierzu zählen die Komponenten Standorterkennung (Netzwerkverbindungen), HIPS, LANDesk Firewall und Gerätesteuerung. Wählen Sie die Einstellungen aus, die Sie auf Zielgeräten bereitstellen möchten, ändern Sie eine vorhandene Einstellung, indem Sie diese auswählen und auf **Bearbeiten** klicken, oder erstellen Sie eine neue Einstellung, indem Sie auf **Konfigurieren > Neu** klicken.
- **Antivirus:** Gibt für Scan-Tasks verwendete Antivirus-Einstellungen an. Mithilfe der Antivirus-Einstellungen können Sie die Anzeige des LANDesk Antivirus-Symbols in der Symbolleiste des Geräts ein- und ausschalten, die Verfügbarkeit von interaktiven Optionen für Endbenutzer steuern, die Einstellungen in Bezug auf die Aktivierung von E-Mail-Scans und Echtzeitschutz festlegen, die zu scannenden Dateitypen und auszuschließenden Dateien und Ordner auswählen, infizierte Dateien unter Quarantäne stellen, Backups veranlassen und die Durchführung geplanter Antivirusscans und Virendefinitionsdatei-Updates konfigurieren. Wählen Sie eine der Einstellungen aus der Liste aus. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählten Einstellungen zu ändern. Klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen. Weitere Informationen finden Sie unter "Informationen zum Dialogfeld "LANDesk Antivirus-Einstellungen"" auf Seite 781.
- **Windows-Firewall:** Definiert die Windows-Firewalleinstellungen auf Zielgeräten. Hier können Sie die Firewall aktivieren und deaktivieren und Firewalleinstellungen konfigurieren, einschließlich Ausnahmen, Eingangsregeln und Ausgangsregeln (für Dienste, Anschlüsse und Programme).

Informationen zum Dialogfeld "Einstellungen für Sicherheitskomponenten konfigurieren"

Verwenden Sie dieses Dialogfeld zur Verwaltung Ihrer Einstellungen für Sicherheitskomponenten. Dieses Dialogfeld wird von mehreren Sicherheitskomponenten gemeinsam verwendet, da es gemeinsame Steueroptionen enthält.

Nachdem Sie die Einstellungen konfiguriert haben, können Sie sie auf Agentenkonfigurationstasks, Installation- und Updatetasks für Sicherheitskomponenten sowie auf Einstellungsänderungstasks anwenden.

Dieses Dialogfeld enthält folgende Optionen:

- **Neu:** Öffnet das Dialogfeld "Einstellungen", in dem Sie die verschiedenen Optionen konfigurieren können.
- **Bearbeiten:** Öffnet das Dialogfeld "Einstellungen". In diesem Dialogfeld können Sie die ausgewählten Einstellungen bearbeiten.
- **Kopieren:** Öffnet eine Kopie der ausgewählten Einstellungen als Vorlage, die von Ihnen dann bearbeitet und umbenannt werden können. Dies kann sich als nützlich erweisen, wenn Sie Einstellungen geringfügig ändern und für einen bestimmten Zweck speichern möchten.

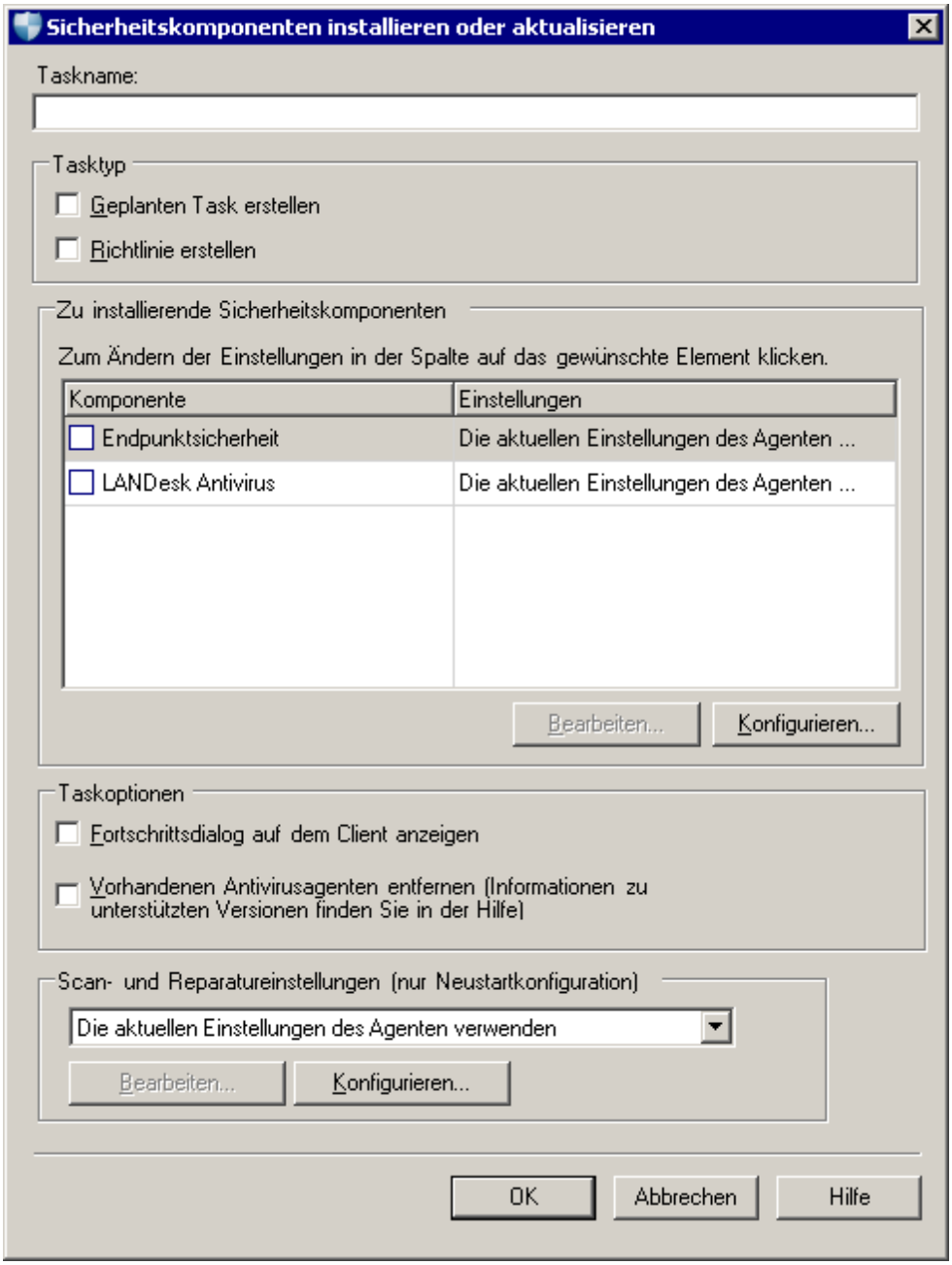
- **Löschen:** Entfernt die ausgewählten Einstellungen aus der Datenbank. (Beachten Sie, dass die ausgewählten Einstellungen möglicherweise mit Tasks oder verwalteten Geräten verknüpft ist. Wenn Sie diese Einstellung löschen, verfügen Geräte mit dieser Einstellung weiterhin über diese Einstellung und verwenden sie auch nach wie vor, bis ein neuer Task vom Typ "Einstellungen ändern" bereitgestellt wird. Geplante Tasks mit dieser Einstellung werden weiterhin auf Zielgeräten ausgeführt, genauso wie Local Scheduler-Tasks mit diesen Einstellungen. Auch sie werden solange ausgeführt, bis eine neue Konfiguration bereitgestellt wird.)
- **Ausgewählte verwenden:** Zeigt an, dass die derzeit ausgewählten Einstellungen für den Task verwendet werden.
- **Schließen:** Schließt das Dialogfeld, ohne Einstellungen auf den Task anzuwenden.

Erstellen eines Tasks zum Installieren oder Aktualisieren von Sicherheitskomponenten

Wenn Sie Sicherheitskomponenten auf verwalteten Geräten installieren oder aktualisieren möchten, können Sie hierfür ebenfalls einen separaten Task verwenden.

So erstellen Sie einen Task zum Installieren oder zum Aktualisieren von Sicherheitskomponenten

1. Klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Agenteneinstellungen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten installieren/aktualisieren**.



3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.

5. Wählen Sie die Komponente aus, die installiert werden soll. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken.
6. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster von Zielgeräten anzeigen möchten, wählen Sie die Option **Fortschrittsdialog auf dem Client anzeigen** aus.
7. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste aus, um deren Neustartkonfiguration (Option "Nur Neustartkonfiguration") auf die Agentenkonfiguration anzuwenden, die Sie erstellen möchten. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Denken Sie daran, dass *nur diejenigen Neustartoptionen*, die Sie unter den von Ihnen ausgewählten Scan- und Reparatureinstellungen angegeben haben, von der Agentenkonfiguration dieser Endpunktsicherheit-Agentenbereitstellung auf Zielgeräten verwendet werden. Sie können vorhandene Scan- und Reparatureinstellungen verwenden, die bereits die gewünschte Neustartkonfiguration beinhalten, oder Sie können komplett neue Scan- und Reparatureinstellungen speziell für Ihre Agentenbereitstellung erstellen.
8. Klicken Sie auf **OK**.

Hilfe zum Installieren und Aktualisieren von Sicherheitskomponenten

Informationen zum Dialogfeld für den Task "Sicherheitskomponenten installieren oder aktualisieren"

Verwenden Sie dieses Dialogfeld, um einen Task zu erstellen und zu konfigurieren, der die Sicherheitskomponenten (über den gemeinsam verwendeten Agenten für Endpunktsicherheit) auf Zielgeräten installiert, auf denen er bisher noch nicht installiert war, oder um einen Task zu erstellen, der die vorhandene Version der Sicherheitskomponenten auf Zielgeräten aktualisiert.

HINWEIS: die Installation wird vom Sicherheitsscanner ausgeführt.

Dieser Task ermöglicht es Ihnen, die Sicherheitskomponenten (und damit verbundene Einstellungen) für ein Gerät auf bequeme Weise bereitzustellen und zu aktualisieren, ohne eine vollständige Agentenkonfiguration neu bereitstellen zu müssen.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Geben Sie zur Identifizierung des Tasks einen eindeutigen Namen ein.
- **Geplanten Task erstellen:** Fügt den Task dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Richtlinie erstellen:** Fügt den Task als Richtlinie dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **Zu installierende Sicherheitskomponenten:** Gibt an, welche Sicherheitskomponenten mit dem Task installiert werden. Markieren Sie die Komponente, die installiert werden soll. Klicken Sie in die Spalte **Einstellungen**, um eine vorhandene Einstellung auszuwählen. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählten Einstellungen zu ändern. Klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen.
- **Fortschrittsdialog auf dem Client anzeigen:** Gibt an, ob im Dialogfeld des Sicherheitsscanners der Fortschritt des Installationsprozesses auf Zielgeräten angezeigt wird.

- **Vorhandenen Antivirus-Agenten entfernen:** Entfernt vor dem Installieren von LANDesk Antivirus automatisch andere Antivirus-Produkte, die möglicherweise bereits auf den Geräten installiert sind (siehe unten). (**HINWEIS:** Sie können vorhandene Antivirus-Produkte auch beim erstmaligen Konfigurieren eines Agenten auf verwalteten Geräten entfernen.)
- **Scan- und Reparatureinstellungen (nur Neustart):** Gibt die Scan- und Reparatureinstellungen an, die dieser spezifischen Installation zugeordnet sind. Der Task verwendet NUR die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten während der Installation.

Liste der Antivirusprodukte von Drittanbietern, die automatisch entfernt werden können

Die aktuelle Liste im Hauptabschnitt zu LANDesk Antivirus finden Sie unter "LANDesk Antivirus" auf Seite 751.

Erstellen eines Tasks zum Entfernen von Sicherheitskomponenten

Wenn Sie Sicherheitskomponenten von verwalteten Geräten entfernen möchten, können Sie hierfür auch einen separaten Task in der Konsole verwenden.

So erstellen Sie einen Task zum Entfernen von Sicherheitskomponenten

1. Klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Agenteneinstellungen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten entfernen**.
3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.
5. Wählen Sie die Komponente aus, die entfernt werden soll.
6. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster des Zielgeräts anzeigen möchten, aktivieren Sie die Option **Fortschrittsdialog auf dem Client anzeigen**.
7. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste der verfügbaren Einstellungen aus, um deren Neustartkonfiguration auf den Task anzuwenden, die Sie gerade erstellen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Der Task verwendet NUR die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten beim Entfernen des Agenten.
8. Klicken Sie auf **OK**.

Hilfe zum Entfernen von Sicherheitskomponenten

Informationen zum Dialogfeld für den Task "Sicherheitskomponenten entfernen"

Dieses Dialogfeld verwenden Sie, um einen Task zu erstellen und zu konfigurieren, der die Sicherheitskomponenten von Zielgeräten entfernt.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Geben Sie zur Identifizierung des Tasks einen eindeutigen Namen ein.
- **Geplanten Task erstellen:** Fügt den Task dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
- **Richtlinie erstellen:** Fügt den Task als Richtlinie dem Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **Zu entfernende Sicherheitskomponenten:** Gibt an, welche Sicherheitskomponenten mit dem Task entfernt werden. Wählen Sie die Komponente aus, die entfernt werden soll.
- **Fortschrittsdialog auf dem Client anzeigen:** Gibt an, ob im Dialogfeld des Sicherheitsscanners beim Entfernen des Agenten von Zielgeräten die Statusanzeige eingeblendet wird.
- **Scan- und Reparatureinstellungen (nur Neustart):** Gibt die Scan- und Reparatureinstellungen an, die diesem spezifischen Vorgang zum Entfernen eines Agenten zugeordnet sind. Der Task verwendet NUR die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten beim Entfernen des Agenten.

Hilfe zu den Listen der vertrauenswürdigen Dateien

Informationen zum Dialogfeld "Liste der vertrauenswürdigen Dateien"

Verwenden Sie dieses Dialogfeld zur Verwaltung Ihrer Listen der vertrauenswürdigen Dateien. Listen der vertrauenswürdigen Dateien umfassen Dateien, die mit einem bestimmten Satz von Rechten (Berechtigungen oder Autorisierungen) konfiguriert wurden, die die Ausführung bestimmter Aktionen für diese Datei *durch* eine Anwendung zulässt oder verweigert.

Dieses Dialogfeld enthält folgende Optionen:

- **Name:** Kennzeichnet die Liste der vertrauenswürdigen Dateien durch einen eindeutigen Namen. Mit der Funktion **Suchen** können Sie in einer Liste nach Elementen suchen, die ein bestimmtes Wort oder einen bestimmten Ausdruck enthalten. Die Ergebnisliste zeigt nur die Elemente an, die Ihren Suchkriterien entsprechen.
- **Hinzufügen:** Öffnet ein Datei-Explorer-Dialogfeld, in dem Sie eine Datei, die Sie mit Dateizertifizierungen konfigurieren möchten, suchen und auswählen können.
- **Bearbeiten:** Hiermit können Sie die Zertifizierungen der ausgewählten Datei bearbeiten.
- **Löschen:** Löscht die ausgewählte Datei und deren Zertifizierungen.
- **Verschieben:** Öffnet ein Dialogfeld, in dem Sie eine oder mehrere vertrauenswürdige Dateien auswählen und in eine andere Liste verschieben oder kopieren können.
- **Als Standard festlegen:** Ordnet diese Liste als die Standardliste der vertrauenswürdigen Dateien für Tasks zu, die diese HIPS- (oder Firewall-)Einstellung verwenden.
- **Kennung:** Identifiziert diese spezifische Liste. Diese Information wird in der Datenbank gespeichert und kann zur Nachverfolgung der einzelnen Listen verwendet werden.

Informationen zum Dialogfeld "Vertrauenswürdige Datei"

Dieses Dialogfeld verwenden Sie zum Konfigurieren von HIPS- und/oder LANDesk Firewall-Rechten für eine bestimmte Anwendungsdatei.

Dieses Dialogfeld enthält folgende Optionen:

- **Dateiname:** Kennzeichnet die Anwendungsdatei, der Zertifizierungen zugewiesen werden.
- **Vollständiger Pfad:** Gibt den Speicherort der Datei an.
- **Dateigröße:** Gibt die Größe der Datei (in KB) an.

- **Dateidatum:** Gibt Erstellungsdatum und -uhrzeit der Datei an.
- **Version:** Gibt die Versionsnummer der Datei an (sofern verfügbar).
- **Zertifiziert:** Gibt Datum und Uhrzeit an, zu der die Zertifizierungen für die Datei erstellt oder zuletzt geändert wurden.
- **MD5-Hash:** Zeigt das MD5-Hash der Datei. Eine Hash-Datei dient dazu, die Integrität der Datei zu gewährleisten.
- **Beschreibung:** Stellt ein Textfeld zur Verfügung, in das Sie eine Beschreibung für die Datei eingeben können.
- **Gesamten Schutz umgehen:** Gewährt der Anwendungsdatei alle Berechtigungen. Die Datei ist komplett ungefiltert und unüberwacht.
- **Puffer-Überlaufschutz umgehen:** Damit können Sie den Puffer-Überlaufschutz umgehen. Es ist sinnvoll, diese Option für Dateien (Prozesse) zu verwenden, die zertifiziert sind und denen Sie vertrauen.
- **Systemsicherheit**
    - **Ausführbare Dateien ändern:** Gewährt der Anwendung das Recht, andere ausführbare Dateien zu ändern.
    - **Geschützte Dateien ändern:** Gewährt der Anwendung das Recht, geschützte Dateien zu ändern. Sie können eine Liste mit geschützten Dateien generieren, wie zum Beispiel mit den LANDesk Management Suite Geräteagenten.
    - **Geschützte Registrierungsschlüssel ändern:** Gewährt der Anwendung das Recht, geschützte Registrierungsschlüssel zu ändern. Geschützte Schlüssel verhindern Malware-Infektionen.
- **Netzwerksicherheit**
    - **E-Mails senden:** Legt fest, dass die Anwendung E-Mail-Nachrichten senden darf. (**HINWEIS:** HIPS erkennt E-Mail-Client-Standardanwendungen und zertifiziert sie automatisch, sodass sie E-Mails senden können.)
- **Datei auf Datenträger**
    - **Zum Systemstart hinzufügen:** Gewährt der Anwendung das Recht, dem Systemstart Dateien hinzuzufügen.
    - **Ausführung zulassen:** Gestattet die Ausführung der Anwendung (dem Prozess) auf dem Gerät. Bei zertifizierten Dateien ist "Ausführung zulassen" automatisch aktiviert. Wenn eine Dateizertifizierung teilweise Rechte bietet, dann ist die Option "Ausführung zulassen" auch automatisch aktiviert.
- **Erweiterte Sicherheitsregeln**
    - **Anwendung im Speicher schützen:** Forciert den Schutz der Anwendung, während sie im Speicher ausgeführt wird. Die Anwendung kann nicht beendet oder geändert werden.
    - **An untergeordnete Prozesse vererben:** Ordnet allen untergeordneten Prozessen dieselben Dateizertifizierungen (Rechte) zu, die von dieser Anwendung ausgeführt werden. Beispiel: Sie können eine Setup- oder Installations-Ausführungsdatei verwenden, um dieselben Rechte an untergeordnete Prozesse, die vom Setupprogramm gestartet wurden, weiterzugeben.
    - **Autorisiertes Installationsprogramm:** Zeigt an, dass die Anwendung die Softwareinstallation oder -bereitstellung durchführen darf. Dies ist der Fall beim LANDesk Management Suite Softwareverteilungstool und kann auch auf andere Softwareverteilungsanwendungen übernommen werden.

- **Erfassungsoptionen**
  - **Dateirechte für Änderungen sperren. (Keine Aktualisierung von Dateirechten im Erfassungsmodus.):**
  - **Diesen Eintrag nur anhand des Dateinamens abgleichen. (Neu erfassten Dateien mit demselben Dateinamen werden dieselben Rechte zugewiesen.):**
- **OK:** Speichert die Dateizertifizierungen und fügt sie der Liste der zertifizierten Dateien im Hauptdialogfeld "HIPS-Einstellungen" hinzu.
- **Abbrechen:** Speichert das Dialogfeld, ohne die Dateizertifizierungen zu speichern.

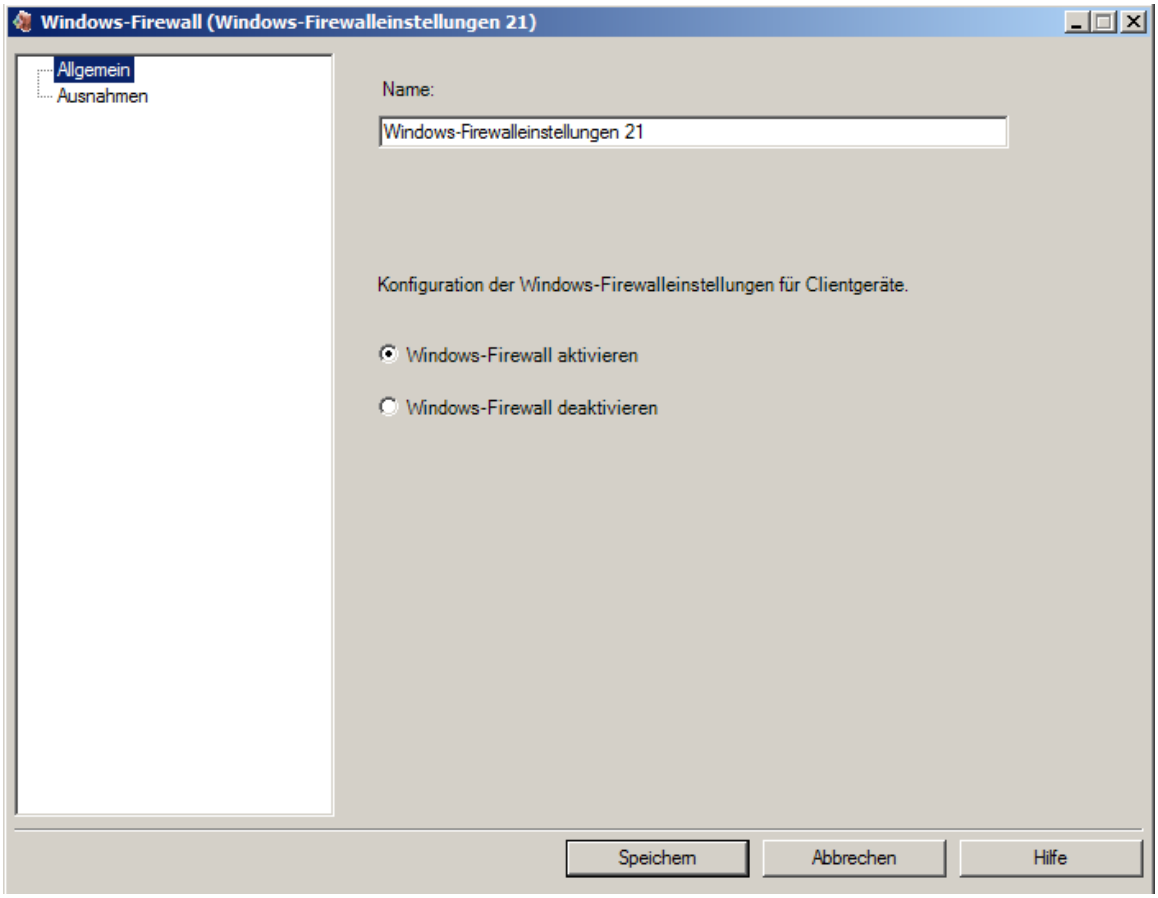
Verwandte Themen

Konfigurieren von Windows-Firewall-Einstellungen

Mit dem Extra "Agenteneinstellungen" können Sie ferner Windows-Firewalleinstellungen erstellen, konfigurieren und bereitstellen, um die Windows-Firewall auf Zielgeräten zu verwalten.

So erstellen Sie Windows-Firewalleinstellungen

1. Klicken Sie auf **Extras > Sicherheit und Compliance > Agenteneinstellungen**.
2. Klicken Sie mit der rechten Maustaste auf **Windows-Firewall**, klicken Sie dann auf **Neu**, wählen Sie die gewünschte Windows-Plattform aus und klicken Sie dann auf **OK**.



Nachdem Sie die Einstellungen konfiguriert haben, können Sie diese über einen Installations- oder Updatetask oder mithilfe eines Tasks zum Ändern von Einstellungen auf verwaltete Geräte übertragen.

Hilfe zur Windows-Firewall

Informationen zum Dialogfeld "Windows-Firewalleinstellungen erstellen"

Dieses Dialogfeld verwenden Sie zur Konfiguration der Windows-Firewalleinstellungen. Windows-Firewalleinstellungen sind mit einem Einstellungsänderungs-Task verknüpft, mit dem Sie die Firewall aktivieren/deaktivieren und Firewalleinstellungen konfigurieren können, einschließlich Ausnahmen, Eingangsregeln und Ausgangsregeln (für Dienste, Ports und Programme).

Sie können diese Funktion verwenden, um eine Konfiguration für die Windows-Firewall auf den folgenden Windows-Versionen bereitzustellen:

- Windows 2003
- Windows XP (SP2 oder neuer)

- Windows Vista

Informationen zur Windows-Firewall (XP/2003): Seite "Allgemein"

Diese Seite verwenden Sie zur Konfiguration der allgemeinen Einstellungen für die Firewall.

Informationen zur Windows-Firewall (XP/2003): Seite "Ausnahmen"

Diese Seite verwenden Sie zum Konfigurieren der Firewallausnahmen.

Dieses Dialogfeld enthält folgende Optionen:

- **Aktuelle Ausnahmen:** Listet Programme, Anschlüsse und Dienste auf, deren Verbindung/Kommunikation *nicht* von der Firewall blockiert wird. Die Firewall verhindert nicht autorisierten Zugriff auf Geräte, mit Ausnahme der Elemente in dieser Liste.
- **Programm hinzufügen:** Ermöglicht Ihnen das Hinzufügen eines bestimmten Programms zur Ausnahmeliste, um die Kommunikation zuzulassen.
- **Port hinzufügen:** Ermöglicht Ihnen das Hinzufügen eines bestimmten Ports zur Ausnahmeliste, um die Kommunikation zuzulassen.
- **Bearbeiten:** Ermöglicht Ihnen die Bearbeitung der Eigenschaften der ausgewählten Ausnahme, einschließlich des Bereichs der betroffenen Geräte.
- **Löschen:** Entfernt die ausgewählte Ausnahme aus der Liste.
- **OK:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Sicherheitsbedrohungsdefinitionen für Windows-Firewall

LANDesk Security Suite bietet vordefinierte Sicherheitsbedrohungsdefinitionen, mit denen Sie die Firewalleinstellungen auf verwalteten Geräten unter bestimmten Windows-Plattformen scannen, erkennen und konfigurieren können. Mit den folgenden Sicherheitsbedrohungsdefinitionen können Sie Firewalleinstellungen scannen und ändern:

- **ST000102:** Sicherheitsbedrohungsdefinition für die Windows-Firewall unter Windows 2003 und Windows XP.
- **ST000015:** Sicherheitsbedrohungsdefinition für die Internetverbindungsfirewall unter Windows 2003 und Windows XP.

Zu den Eigenschaften der Sicherheitsbedrohung der Windows-Firewall gehören benutzerdefinierte Variablen, mit deren Hilfe Sie Windows-Firewalleinstellungen konfigurieren können. Sie können diese Sicherheitsbedrohungsdefinitionen zum Scannen auf Ihre angegebenen Einstellungen verwenden und eine Anfälligkeitsbedingung zurückgeben, falls diese Einstellungen nicht übereinstimmen. Die benutzerdefinierte Definition können Sie dann in einem Reparaturtask dazu verwenden, die Firewall ein- oder auszuschalten oder die Firewalleinstellungen auf dem gescannten Gerät neu zu konfigurieren.

Informationen zur Windows-Firewall (Vista): Seite "Allgemeine Regeln"

Diese Seite verwenden Sie zum Konfigurieren der allgemeinen Regeln für die Firewall.

Informationen zur Windows-Firewall (Vista): Eingangsregeln

Diese Seite verwenden Sie zum Konfigurieren der Eingangsregeln für die Firewall.

Informationen zur Windows-Firewall (Vista): Ausgangsregeln

Diese Seite verwenden Sie zum Konfigurieren der Ausgangsregeln für die Firewall.

Generieren von Sicherheitsautorisierungscodes

Dieses Dialogfeld verwenden Sie zur Erstellung eines Autorisierungscodes, der es einem Endbenutzer gestattet, eine blockierte Operation für eine kurze Zeitspanne auszuführen. Sie können einen Autorisierungscode dazu verwenden, einem bestimmten Benutzer oder einem IT-Administrator temporär Zugriff auf ein verwaltetes Gerät zu geben.

Wenn zum Beispiel ein Benutzer versucht, ein USB-Gerät anzuschließen, das aufgrund von Einstellungen zur Gerätesteuerung nicht zulässig ist, wird auf dem Gerät des Endbenutzers eine Popupmeldung mit einem Operationscode angezeigt. Der Benutzer würde diesen Operationscode dann an den Administrator weiterreichen, der diesen zur Generierung eines Autorisierungscode verwendet, den er wiederum an den Endbenutzer zurückreicht. Dies ermöglicht es ihm, besagte Aktion auf temporärer Basis auszuführen.

So generieren Sie einen Autorisierungscode

1. Klicken Sie im Extra **Agenteneinstellungen** auf die Symbolleistenschaltfläche **Einstellungen konfigurieren** und klicken Sie dann auf **Autorisierungscode generieren**.
2. Geben Sie den vom Endbenutzer gelieferten Operationscode ein.
3. Wenn der Operationscode gültig ist, wird automatisch ein Autorisierungscode generiert.
4. Geben die den Typ des Vorgangs ein, den der Benutzer ausführen möchte.
5. Reichen Sie den neuen Autorisierungscode an den Benutzer weiter. Der Benutzer gibt diesen Autorisierungscode dann bei der entsprechenden Aufforderung ein, um den blockierten Vorgang auszuführen.

VORSICHT: Nicht korrekte Popup-Meldung
Wenn einem Benutzer mittels Autorisierungscode Zugriff gewährt wird, kann es sein, dass eine Popup-Meldung auf dem Gerät des Endbenutzers angezeigt wird, die darauf hindeutet, das HIPS deaktiviert wurde, unabhängig davon, welche Aktion der Benutzer tatsächlich ausgeführt hat. Diese Meldung kann ignoriert werden.

Sicherheitsaktivität

Sicherheitsaktivität – Übersicht

Das neue Extra **Sicherheitsaktivität** bietet ein praktisches separates Extra für die Anzeige von Status- und Aktivitätsinformationen zu mehreren LANDesk Security Suite Diensten, die auf Ihren verwalteten Geräten ausgeführt werden.

Mit "Sicherheitsaktivität" können Sie Status- und Aktivitätsinformationen zu folgenden Funktionen anzeigen:

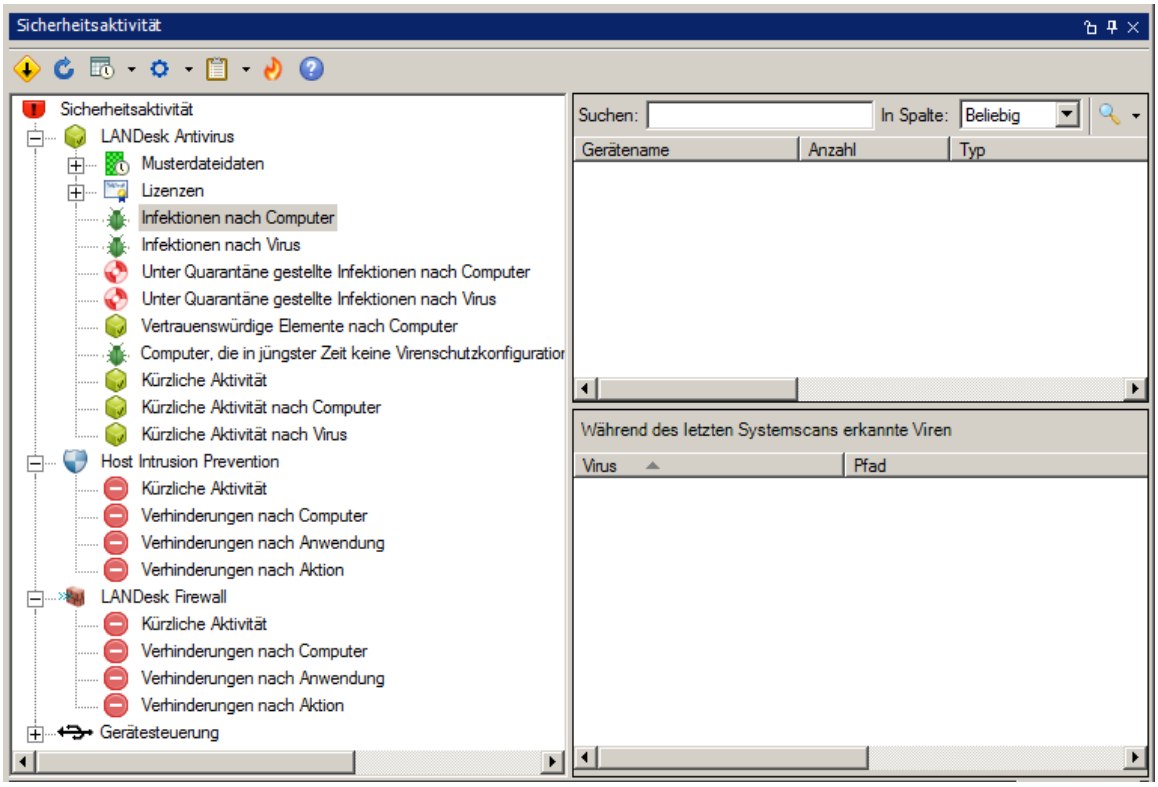
- LANDesk Antivirus
- Host Intrusion Prevention (HIPS):
- LANDesk Firewall
- Gerätesteuerung

Außerdem können Sie damit die folgenden Tasks ausführen.

- Grenzwerteinstellungen für Sicherheitsaktivität konfigurieren
- Sicherheitsaktivitätsinformationen löschen

Anzeigen von Sicherheitsstatus und Sicherheitsaktivität

Mit dem Extra "Sicherheitsaktivität" können Sie Informationen zu LANDesk Security Suite Diensten anzeigen.



Die Sicherheitsextras, die Sie anzeigen können, werden in den folgenden Abschnitten beschrieben.

Anzeigen der LANDesk Antivirus-Aktivität und -Statusinformationen

Wenn der LANDesk Antivirus-Scanner eine der ausgewählten Virendefinitionen auf einem Zielgerät erkennt, wird diese Information an den Coreserver weitergegeben. Sie können sich einer der folgenden Methoden bedienen, um nach Abschluss eines Scans erkannte Sicherheitsdaten anzuzeigen.

In diesem Fenster wird die Antivirusaktivität und Statusinformationen nach den folgenden Kategorien geordnet angezeigt:

- Infektionen nach Computer
- Infektionen nach Virus
- Unter Quarantäne gestellte Infektionen nach Computer
- Unter Quarantäne gestellte Infektionen nach Virus
- Vertrauenswürdige Elemente nach Computer
- Computer, die in jüngster Zeit nicht Bericht erstattet haben
- Kürzlich durchgeführte Virenschutzaktivität nach Computer
- Kürzliche Virenschutzaktivität nach Virus

Außerdem können Sie für ein gescanntes Gerät mit der rechten Maustaste auf das Gerät klicken, **Sicherheits- und Patchinformationen** auswählen und dann in der Dropdownliste **Typ** die Option **Antivirus** auswählen. Sie können Folgendes anzeigen:

- Fehlende Antivirus-Updates
- Installierte Antivirus-Updates
- Reparaturverlauf löschen

Informationen zum Dialogfeld "Antivirus-Aktivität und Statusinformationen"

Verwenden Sie dieses Dialogfeld, um detaillierte Antivirus-Aktivitäten und Statusinformationen für alle verwalteten Geräte, auf denen der LANDesk Antivirus-Agent installiert ist, anzuzeigen. Diese Ergebnisdaten des Scans werden zum Generieren der im Tool **Berichte** bereitgestellten LANDesk Antivirus-Berichte verwendet.

Um Bereich und Fokus der angezeigten Daten anzupassen, klicken Sie auf **Grenzwerte** und ändern die Zeitspannen-Grenzwerte für die jüngsten Virenschutzaktivitäten gescannter Geräte und für Geräte, die in jüngster Zeit nicht gescannt wurden.

Sie können auch mit der rechten Maustaste auf ein Gerät in dieser Ansicht klicken, um das Kontextmenü zu öffnen und verfügbare Tasks direkt auszuführen.

Dieses Dialogfeld enthält folgende Optionen:

- **Aktualisieren:** Aktualisiert die Felder im Dialogfeld mit den neuesten Antivirus-Scan-Informationen aus der Datenbank.
- **Grenzwerte:** Öffnet das Dialogfeld **Grenzwerteinstellungen**. In diesem Dialogfeld können Sie die Dauer (in Tagen) für Antivirus-Aktivitäten in jüngster Zeit und für Antivirus-Scans vom Typ "nicht in jüngster Zeit gescannt" festlegen. Grenzwerte bestimmen den Zeitraum, für den Antivirus-Scan-Ergebnisse erfasst und in den zwei computerspezifischen Anzeigekategorien eingeblendet werden.
- **Infektionen nach Computer:** Listet im rechten Fensterausschnitt Geräte auf, auf denen während des letzten Systemscans Vireninfektionen erkannt wurden. Wählen Sie ein Gerät aus, um zu erfahren, mit welchen Viren das Gerät infiziert ist.

- **Infektionen nach Virus:** Listet im rechten Fensterausschnitt Viren auf, die während des letzten Systemscans auf verwalteten Geräten erkannt wurden. Wählen Sie eine Virendefinition aus, um zu erfahren, welche Geräte mit dem Virus infiziert wurden.
- **Computer, die nicht in jüngster Zeit auf Anfälligkeiten gescannt wurden:** Listet alle Geräte mit installiertem LANDesk Antivirus-Agent auf, die innerhalb des im Dialogfeld **Grenzwerteinstellungen** angegebenen Zeitraums nicht auf Viren gescannt wurden. Wenn Sie einen sofortigen Antivirus-Scan ausführen möchten, klicken Sie mit der rechten Maustaste auf das Gerät, klicken Sie auf **LANDesk Antivirus - Jetzt scannen**, wählen Sie eine Antivirus-Einstellung aus und klicken Sie dann auf **OK**.
- **Computer, auf denen in jüngster Zeit Virenschutzaktivität registriert wurde:** Listet alle Geräte mit installiertem LANDesk Antivirus-Agent auf, die innerhalb des im Dialogfeld **Grenzwerteinstellungen** angegebenen Zeitraums auf Viren gescannt wurden und Virenschutzaktivität zurückgegeben haben. Wählen Sie ein Gerät aus, um die spezifischen Antivirus-Aktivitäten dieses Geräts einzublenden: Virenerkennung, Entfernen von Viren, Isolieren infizierter Objekte in einem Quarantäneordner, Backup und Wiederherstellung.

Anzeigen der HIPS-Aktivität

Wenn HIPS Verletzungen seiner Regeln und Zertifizierungsrechte erkennt, werden diese Informationen dem Coreserver gemeldet. Erkannte HIPS-Aktivität kann mithilfe der folgenden Methoden angezeigt werden:

Informationen zur netzwerkweiten HIPS-Aktivität erhalten Sie, indem Sie im Extra "Sicherheitsaktivität" die Gruppe **Host Intrusion Prevention** öffnen. Im Fenster werden HIPS-Aktivitäten nach folgenden Kategorien sortiert angezeigt:

- Verhinderungen nach Computer
- Verhinderungen nach Anwendung
- Verhinderungen nach Aktion

Sie können auch spezifische Host Intrusion-Aktivitäten, einschließlich folgender Details, am unteren Rand des Fensters einblenden:

- Aktionsdatum
- Aktion
- Beschreibung
- Anwendung
- Dateiversion
- Dateigröße
- Dateidatum
- Modus
- MD5-Hash

Informationen zum Dialogfeld "HIPS-Aktivität"

Verwenden Sie dieses Dialogfeld, um detaillierte HIPS-Aktivitäten für alle verwalteten Geräte, auf denen der LANDesk HIPS-Agent installiert ist, anzuzeigen. Diese Daten werden zum Generieren der im Tool **Berichte** bereitgestellten LANDesk HIPS-Berichte verwendet.

Um Umfang und Fokus der angezeigten Daten anzupassen, klicken Sie auf **Grenzwerte** und ändern das Grenzwertintervall für die Speicherung von HIPS-Aktivitätsdaten in der Coredatenbank und für die Anzahl anzuzeigender Elemente in den Listen im HIPS-Aktivitätsfenster.

Sie können auch mit der rechten Maustaste auf ein Gerät in dieser Ansicht klicken, um das Kontextmenü zu öffnen und verfügbare Tasks direkt auszuführen.

Dieses Dialogfeld enthält folgende Optionen:

- **Aktualisieren:** Aktualisiert die Felder im Dialogfeld mit den neuesten HIPS-Informationen aus der Datenbank.
- **Grenzwerte:** Öffnet das Dialogfeld **Grenzwerteinstellungen**. In diesem Dialogfeld können Sie den Zeitraum (in Tagen) für die Speicherung von HIPS-Daten in der Coredatenbank und die Anzahl der anzuzeigenden Elemente in den HIPS-Aktivitätslisten definieren.
- **Entfernen:** Entfernt HIPS-Aktivitätsdaten vollständig und dauerhaft sowohl aus diesem Anzeigefenster als auch aus der Coredatenbank.
- **Verhinderungen nach Computer:** Listet im rechten Fensterausschnitt Geräte auf, auf denen HIPS-Verletzungen aufgedeckt wurden. Wählen Sie ein Gerät aus, um zu überprüfen, um welche Verletzungen es sich im Einzelnen handelt.
- **Verhinderungen nach Anwendung:** Listet im rechten Fensterausschnitt Anwendungen auf, die auf verwalteten Geräten erkannt wurden. Wählen Sie eine Anwendung aus, um nachzuprüfen, auf welchen Geräten sie erkannt wurde.
- **Verhinderungen nach Aktion:** Listet im rechten Fensterausschnitt Aktionen auf, die auf verwalteten Geräten ausgeführt wurden. Wählen Sie eine Aktion aus, um nachzuprüfen, für welche Geräte sie ausgeführt wurde.

Anzeigen der LANDesk Firewallaktivitäten

In diesem Fenster werden Firewallaktivitäten nach folgenden Kategorien sortiert angezeigt:

- Verhinderungen nach Computer
- Verhinderungen nach Anwendung
- Verhinderungen nach Aktion

Anzeigen der Gerätesteuerungsaktivitäten

In diesem Fenster werden Aktivitäten der Gerätesteuerung nach folgenden Kategorien sortiert angezeigt:

- Blockierte Speichergeräte
- Blockierte CD/DVD-Geräte
- Sonstige blockierte Geräte
- Schattenkopien von Dateien

Grenzwerteinstellungen für Sicherheitsaktivität konfigurieren

Informationen zur Sicherheitsaktivität Ihrer verwalteten Geräte können sich sehr schnell ansammeln und die Leistung der Coredatenbank beeinträchtigen.

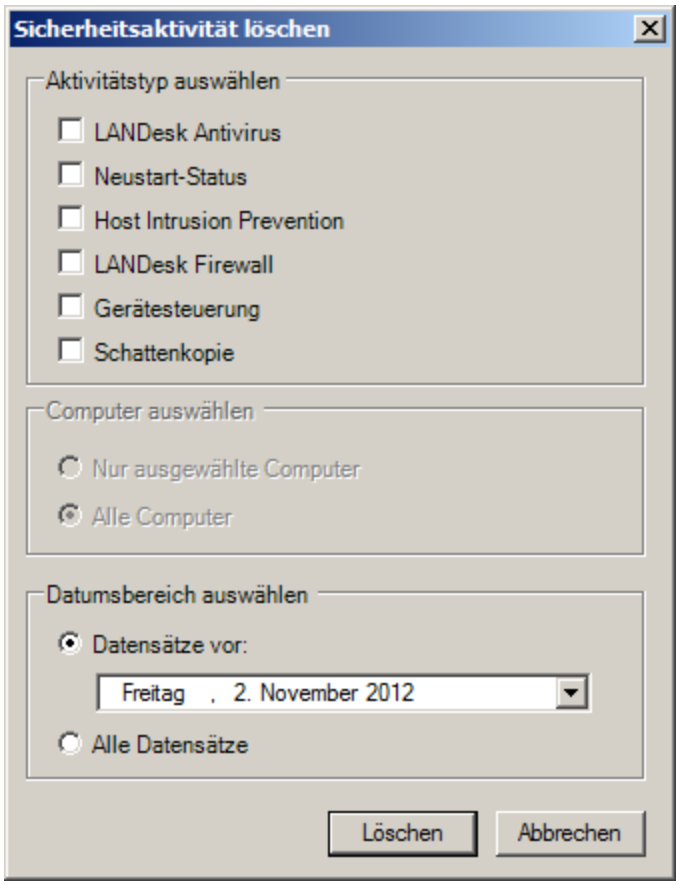
Dieses Dialogfeld verwenden Sie, um die Zeitfenster für die Datensammlung zu definieren und die Menge der sicherheitsbezogenen Daten zu steuern, die in der Coredatenbank für die LANDesk Extras "Antivirus", "HIPS" und "Firewall" gespeichert werden. Diese Informationen werden in den entsprechenden Ansichten zur Sicherheitsaktivität angezeigt.

Informationen zum Dialogfeld "Grenzwerteinstellungen"

- **Allgemeine Grenzwerte**
  - **Grenzwert für Ansichten zur Aktivität in jüngster Zeit:** Gibt den Zeitraum (in Tagen) an, über den Informationen zur Sicherheitsaktivität für Geräte erfasst werden, die gescannt wurde und Virenschutzaktivität zurückgemeldet haben.
  - **Beim Anzeigen von Ergebnissen die Liste kürzen auf:** Gibt die maximal zulässige Anzahl Einträge an, die in den Listen in den Aktivitätsdialogfeldern unterstützt wird. Sie können 1 bis 999.999 Elemente angegeben.
- **LANDesk Antivirus:**
  - **Musterdateien sind veraltet, wenn sie älter sind als:**
  - **Grenzwert für Lizenzablaufwarnung:**
  - **Grenzwert für "Nicht kürzlich gescannt":** Gibt den Zeitraum (in Tagen) an, über den Geräteinformationen für mit Antivirus konfigurierten Geräte erfasst werden, die nicht gescannt wurden.
- **Automatisch löschen (nur HIPS / LANDesk Firewall):**
  - **Aktivitäten automatisch löschen, wenn sie älter sind als:** Gibt an, für wie viele Tage gemeldete HIPS-Aktivitäten und LANDesk Firewallaktivitäten für geschützte Geräte maximal in der Coredatenbank aufbewahrt werden sollen. Sie können 1 bis 999 Tage angegeben. (**WICHTIG**: LANDesk empfiehlt, sorgsam darauf zu achten, wie viele Daten an den Core gesendet werden und eine optimale Anzahl von Tagen zu ermitteln, damit HIPS-Daten den Speicher nicht zu stark beanspruchen oder die Leistung der Coredatenbank beeinträchtigen.)

Löschen der Sicherheitsaktivität

Von Zeit zu Zeit sollten Sie die Informationen zur Sicherheitsaktivität für die verschiedenen Komponenten löschen. Sie können dies im Extra "Sicherheitsaktivität" mithilfe der Symbolleistenschaltfläche **Aktivität löschen** tun.



Das Löschen der Sicherheitsaktivität ist ein einmaliger Task, kein geplanter Task und auch keine Richtlinie.

Informationen zum Dialogfeld "Sicherheitsaktivität löschen"

Dieses Dialogfeld verwenden Sie, um sämtliche Aktivitätsdatensätze aus der Konsole und aus der Coredatenbank zu löschen.

Dieses Dialogfeld enthält folgende Optionen:

- **Aktivitätstyp auswählen:** Gibt die Sicherheitskomponenten an, deren Aktivitätsinformationen Sie löschen möchten.
- **Computer auswählen:** Gibt an, für welche verwalteten Geräte die Sicherheitsaktivitätsdaten gelöscht werden. (Hinweis: Sie müssen Administratorrechte besitzen, um diesen Task ausführen zu können.)
- **Datumsbereich auswählen:** Gibt das früheste Datum an, ab dem Sicherheitsaktivitätsdaten gelöscht werden. Sie können aber auch einfach die Option **Alle Datensätze** verwenden, um sämtliche vorhandenen Aktivitätsdaten zu löschen.
- **Entfernen:** Entfernen die Aktivitätsdatensätze für die von Ihnen ausgewählten Komponenten vollständig.

Konfigurieren von Sicherheitsalarmeinstellungen

Sie können sicherheitsbezogene Alarme konfigurieren, damit Sie benachrichtigt werden, wenn bestimmte Ereignisse auf verwalteten Geräten in Ihrem System erkannt werden. Die Sicherheitskomponente Antivirus verwendet hierzu das Standard-Alarmtool von LANDesk.

Das Dialogfeld für Alarmeinstellungen enthält sowohl Optionen für Anfälligkeitsalarme als auch Optionen für Antivirusalarme.

Antivirusalarme

Die Antivirus-Alarmeinstellungen sind auf der Registerkarte **Antivirus** des Dialogfelds **Alarmeinstellungen** zu finden.

Sie müssen zuerst die Antivirusalarme im Extra "Alarmeinstellungen" der Konsole konfigurieren. Es gibt u. a. folgende Antivirusalarme:

- Eine Virenschutzaktion, für die ein Alarm generiert werden kann, ist fehlgeschlagen.
- Eine Virenschutzaktion, für die ein Alarm generiert werden kann, wurde erfolgreich ausgeführt.
- Virenausbruch-Alarm (pro Virus)

Folgende Antiviruseregnisse können Antivirusalarme generieren:

- Virusentfernung fehlgeschlagen
- Virusentfernung erfolgreich
- Quarantäne fehlgeschlagen
- Quarantäne erfolgreich
- Löschen fehlgeschlagen
- Löschen erfolgreich

Wählen Sie die gewünschten Alarme aus. Mit der Option "Zeitraum" wird verhindert, dass zu häufig Alarme generiert werden. Wenn innerhalb des angegebenen Zeitraums (für einen beliebigen Antivirusauslöser) mehr als ein Alarm gegeben wird, werden alle Alarme nach dem ersten ignoriert.

Sie können den vollständigen Antivirus-Alarmverlauf im Dialogfeld "Sicherheits- und Patchinformationen" des jeweiligen Geräts einsehen. Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie **Sicherheits- und Patchinformationen** aus. Wählen Sie dann in der Liste "Typ" den Antivirustyp und schließlich das Objekt "Antivirus-Verlauf" aus.

Anfälligkeitsalarme

Informationen zu Anfälligkeitsalarmen finden Sie unter "Konfigurieren von Patch und Compliance-Alarmen" auf Seite 647.

Endpunktsicherheit

Endpunktsicherheit – Übersicht

Bei dem neuen Extra "Endpunktsicherheit" handelt es sich faktisch um eine Kombination aus sich ergänzenden Funktionen und Einstellungen, mit denen Sie ein hohes Maß an Systemsicherheit für die verwalteten Geräte in Ihrem Netzwerk konfigurieren und implementieren können. Sie können Netzwerkverbindungen für verwaltete Geräte und auch den Zugriff anderer Gerätetypen auf diese Geräte beschränken und die Extras "Host Intrusion Prevention System (HIPS)" und "LANDesk Firewall" dazu verwenden, nicht autorisierte Anwendungsvorgänge zu verhindern.

Die Endpunktsicherheit stellt einen undurchdringbaren Abwehrmechanismus für alle geschützten Geräte innerhalb Ihres LANDesk Netzwerks, für die Netzwerkgrenzen sowie für mobile Benutzer dar, indem es Ihnen vollständige Kontrolle über den Zugriff auf diese Geräte, den Zugriff von diesen Geräten und über alles gibt, was auf diesen geschehen darf.

Obwohl die Endpunktsicherheit als ein einziger konsolidierter Agent für Zielgeräte bereitgestellt wird, ist sie vollständig konfigurierbar und stellt Dienste für mehrere Sicherheitskomponenten bereit.

Komponenten der Endpunktsicherheit

Zu den Komponenten der Endpunktsicherheit zählen folgende:

- **Standorterkennung:** Netzwerkverbindungskontrolle mit Standorterkennung und Funktionen für vertrauenswürdigen Speicherort. Weitere Informationen finden Sie unter "Hilfe zur Endpunktsicherheit" auf Seite 716.
- **Host Intrusion Prevention System (HIPS):** Verhinderung von nicht autorisierten Eindringversuchen. Weitere Informationen finden Sie unter "Host Intrusion Prevention System (HIPS) – Übersicht" auf Seite 719.
- **LANDesk Firewall:** Verhinderung von nicht autorisierten Anwendungsvorgängen und -verbindungen. Weitere Informationen finden Sie unter "Konfigurieren der LANDesk Firewalleinstellungen" auf Seite 734.)
- **Gerätesteuerung:** Zugriffsbeschränkungen für Speichervolumes, Geräte, Schnittstellen usw. Weitere Informationen finden Sie unter "Gerätesteuerung – Übersicht" auf Seite 740.
- **Listen der vertrauenswürdigen Dateien:** Listen mit Dateien, die mit einem bestimmten Satz von Rechten (Berechtigungen oder Autorisierungen) konfiguriert wurden, die die Ausführung bestimmter Aktionen für diese Datei *durch* eine Anwendung zulässt oder verweigert.

Mit Endpunktsicherheit können Sie vertrauenswürdige Speicherorte (Netzwerkverbindungen) für verwaltete Geräte definieren, Einstellungen für jede der oben aufgeführten Endpunktsicherheitskomponenten erstellen und diese Einstellungen bereitstellen, je nachdem, ob sich das Gerät innerhalb oder außerhalb des vertrauenswürdigen Netzwerkspeicherorts befindet.

Wie oben erwähnt, handelt es sich bei der Endpunktsicherheit um einen einzigen Agenten, der Schutzregeln auf verwalteten Geräten durchsetzt und die Funktionalität jeder einzelnen Sicherheitskomponente kontrolliert. Die Endpunktsicherheit gibt Ihnen die Flexibilität, die Sicherheitskomponenten unabhängig voneinander oder im Rahmen einer kombinierten Bereitstellung zu aktivieren und zu konfigurieren. So können Sie beispielsweise nur den HIPS-Schutz oder HIPS und Gerätesteuerung (über die jeweiligen Einstellungen) oder jede andere Kombination von Sicherheitskomponenten bereitstellen.

Dieser Abschnitt beschreibt, wie Sie die Endpunktsicherheit auf Ihren verwalteten Geräten aktivieren. Ferner bietet er Ihnen Informationen zu jeder darin enthaltenen Komponente der Endpunktsicherheit.

Aktivieren und Bereitstellen der Endpunktsicherheit

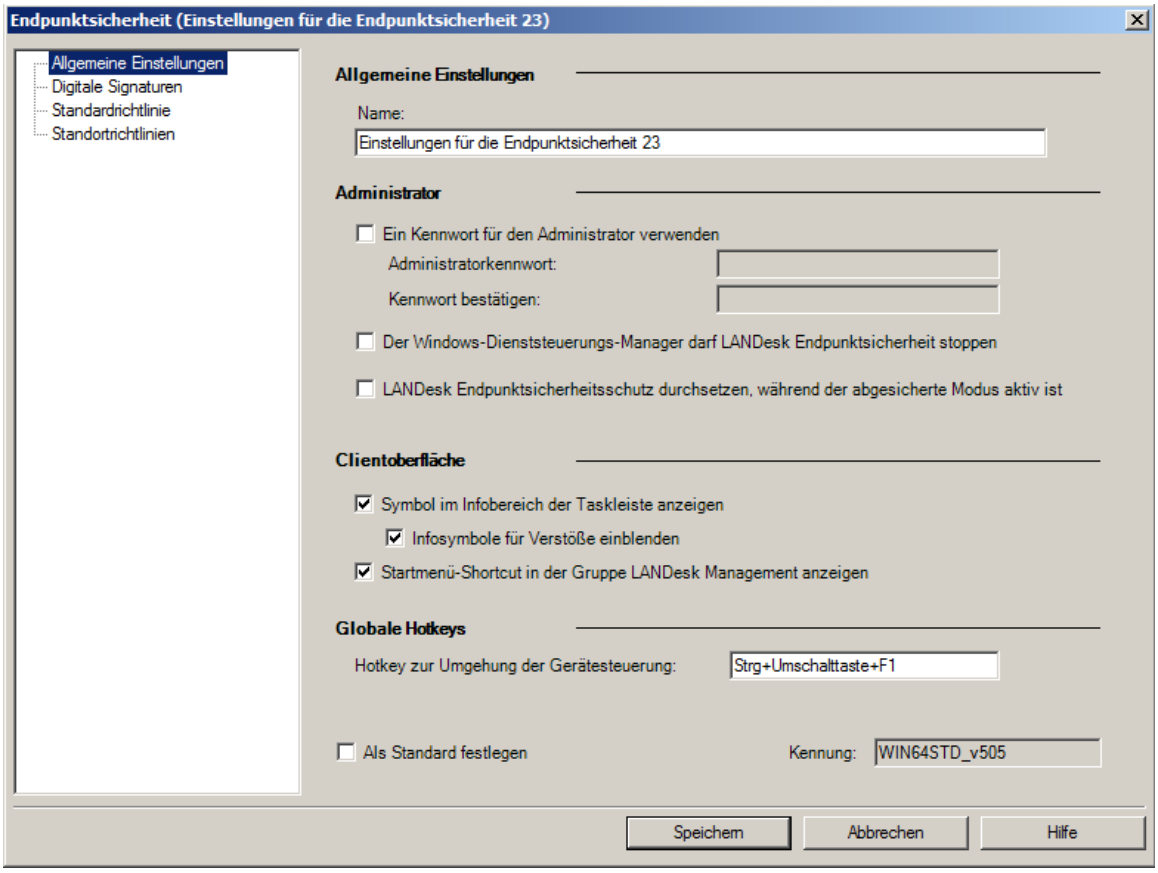
Die Endpunktsicherheit wird durch das Bereitstellen von Einstellungen für die Endpunktsicherheit auf verwalteten Geräten aktiviert.

Die Endpunktsicherheit kann auf verwalteten Geräten über die anfängliche Agentenkonfiguration aktiviert werden. Sie können auch einen Task vom Typ "Einstellungen ändern" verwenden, um Einstellungen für die Endpunktsicherheit auf Zielgeräten zu installieren oder zu aktualisieren.

Erstellen von Einstellungen für die Endpunktsicherheit

So erstellen Sie Einstellungen für die Endpunktsicherheit

1. Klicken Sie im Fenster des Extras **Agenteneinstellungen** mit der rechten Maustaste auf **Endpunktsicherheit** und klicken Sie dann auf **Neu**.



2. Geben Sie auf der Seite **Allgemeine Einstellungen** einen Namen für die Einstellungen ein und geben Sie dann die allgemeinen Anforderungen und Aktionen an. Wenn Sie Informationen zu einer Option benötigen, klicken Sie auf **Hilfe**.

3. Wenn Sie Netzwerkverbindungen verwalten möchten, wählen Sie die Option **Standorterkennung verwenden**. Bei Auswahl dieser Option wird die Seite **Vertrauenswürdiger Speicherort** angezeigt. Wenn Sie diese Option wählen, werden außerdem zwei separate Gruppen auf der Seite **Sicherheitsrichtlinien** verfügbar, eine für den Fall, dass sich das Gerät am vertrauenswürdigen Speicherort befindet und eine zweite für den Fall, dass sich das Gerät außerhalb des vertrauenswürdigen Speicherorts befindet. Wenn die Funktion für die Standorterkennung nicht aktiviert ist, wird nur eine Richtliniengruppe benötigt.
4. Wählen Sie auf der Seite **Sicherheitsrichtlinien** aus, welche Komponenten der Endpunktsicherheit Sie für Zielgeräte mit den Einstellungen für die Endpunktsicherheit bereitstellen möchten.
5. Definieren Sie auf der Seite **Vertrauenswürdiger Speicherort** die zulässigen Netzwerkverbindungen (nach IP-Adresse, IP-Bereich oder Subnetz).
6. Klicken Sie auf **Speichern**.

Nachdem Sie die Einstellungen konfiguriert haben, können Sie diese über einen Installations- oder Updatetask oder mithilfe eines Tasks zum Ändern von Einstellungen auf verwaltete Geräte übertragen.

Was geschieht auf einem Gerät mit Endpunktsicherheit?

In diesem Abschnitt erfahren Sie, wie der Client für Endpunktsicherheit auf verwalteten Geräten angezeigt wird, was auf Endbenutzergeräten geschieht, wenn diese mit Endpunktsicherheit geschützt sind, und welche Aktionen Endbenutzer in die Wege leiten können, wenn eine Sicherheitsverletzung erkannt wird.

Clientbenutzeroberfläche

Sobald Endpunktsicherheit auf verwalteten Geräten bereitgestellt wurde, kann der Client entweder über das Startmenü oder das Taskleistensymbol geöffnet werden.

WICHTIG: Administratorkennwortschutz
Wenn der Administrator die Kennwortschutzoption in den Einstellungen für die Endpunktsicherheit aktiviert hat, muss das korrekte Kennwort eingegeben werden, damit bestimmte Clientfunktionen zur Verfügung gestellt werden.

Taskleistensymbol

Das Taskleistensymbol zeigt an, ob die HIPS-Komponente der Endpunktsicherheit im Erfassungsmodus oder im automatischen Blockiermodus ausgeführt wird.

Mit einem Rechtsklick auf das Symbol können Benutzer das Kontextmenü öffnen und aus folgenden Optionen wählen:

- **Öffnen:** Öffnet den Client.
- **Optionen:** Zeigt die Optionen an, die vom Administrator an der Konsole konfiguriert wurden (schreibgeschützt).
- **Automatikmodus:** Ermöglicht die Ausführung der HIPS-Komponente im Automatikmodus. In diesem Modus werden alle vordefinierten Sicherheitsverletzungen blockiert.
- **Erfassungsmodus:** Ermöglicht die Ausführung der HIPS-Komponente im Erfassungsmodus. In diesem Modus sind alle Sicherheitsverletzungen zulässig, doch werden sie überwacht und in einer Aktionsverlaufsdatei erfasst.

- **Software installieren:** Öffnet ein Datei-Explorer-Fenster, in dem Benutzer ein auszuführendes Installations- oder Setup-Programm auswählen können.
- **Entladen:** Hiermit können Benutzer den Client auf ihrem Computer deinstallieren.

Endbenutzeraktionen

Der Client zeigt ein Fenster an, das dem Benutzer folgende Möglichkeiten bietet:

- Anzeige des Aktivitätsprotokolls.
- Anzeige der Optionen, die vom Administrator an der Konsole konfiguriert wurden (schreibgeschützt).
- Auf der Seite **Status**: Zeigen Sie Komponenteninformationen (zu HIPS, zur Positivliste, zur Firewall und zur Gerätesteuerung), den aktuellen Betriebsmodus und die auf dem Client stattfindenden Aktivitäten an. Ändern Sie den Betriebsmodus (hierzu kann ein Autorisierungskennwort erforderlich sein).
- Auf der Seite **Programme**: Zeigen Sie aktive Anwendungen und ihre Autorisierungen an. Wählen Sie Programme aus und zeigen Sie deren Autorisierungen an oder beenden Sie den Prozess. Ändern Sie Anzeigeoptionen.
- Auf der Seite **Startup**: Zeigen Sie den Inhalt des System-Startups an und ändern Sie ihn. Darüber hinaus können Sie auf dem Client ausgeführte Dienste und Internet Explorer-Erweiterungen anzeigen und bearbeiten.
- Auf der Seite **Schutz**: Zeigen Sie Programmzugriffsrechte und Ordnerschutzeinstellungen an. Erstellen, bearbeiten und löschen Sie Dateischutzregeln und ändern Sie die Priorität von Regeln in der geordneten Liste.
- Auf der Seite **Zertifizierungen**: Zeigen Sie Programme mit speziellen Dateizertifizierungen an. Fügen Sie Dateizertifizierungen hinzu und löschen Sie sie.

Hilfe zur Endpunktsicherheit

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten von Einstellungen für die Endpunktsicherheit.

Dieses Dialogfeld umfasst die folgende Seiten:

- "Informationen zur Endpunktsicherheit: Seite "Allgemeine Einstellungen"" auf Seite 716
- "Hilfe zur Endpunktsicherheit" auf Seite 716
- "Informationen zur Endpunktsicherheit: Standardrichtlinie" auf Seite 718
- "Informationen zur Endpunktsicherheit: Seite "Standortrichtlinien"" auf Seite 718

Informationen zur Endpunktsicherheit: Seite "Allgemeine Einstellungen"

Diese Seite verwenden Sie für die Konfiguration der Standorterkennung (vertrauenswürdiges Netzwerk) und anderen Zugriffseinstellungen.

- **Name:** Kennzeichnet die Einstellungen mit einem eindeutigen Namen.
- **Standorterkennung verwenden:** Dient der Verwaltung von Netzwerkverbindungen. Sie können die Netzwerk-IP-Adressen beschränken, zu denen Geräte Verbindungen herstellen dürfen. Durch die Angabe der zulässigen Netzwerkadressen konfigurieren Sie die Netzwerkbeschränkungen. Das Gerät kann nur IP-Adressen in einem bestimmten, ausdrücklich zulässigen Adressenbereich empfangen.
- **Windows Service Control Manager darf den Dienst "Endpunktsicherheit" stoppen:** Benutzer können den Dienst "Endpunktsicherheit" auf dem Client stoppen.

- **Administratorkennwort:** Gibt das Kennwort an, das auf mit diesen Einstellungen für die Endpunktsicherheit konfigurierten Geräten erforderlich ist, um bestimmte Aktionen auf dem geschützten Gerät ausführen zu können. Folgende Aktionen erfordern ein Kennwort: der Zugriff auf die HIPS-Clientbenutzeroberfläche, die Installation nicht signierter Software, die Genehmigung von HIPS-Verletzungen, das Entladen von HIPS, das Löschen des lokalen Berichts und der Wechsel des HIPS-Betriebsmodus.
- **Optionen für die Client-Benutzeroberfläche:** Gibt an, wie der Client für die Endpunktsicherheit auf verwalteten Geräten angezeigt wird.
    - **Infobereichsymbol einblenden:** Blendet das Infobereichsymbol in der Clientschnittstelle ein.
    - **Verletzungs-Popupmeldungen anzeigen:** Zeigt eine Meldung auf dem Endbenutzergerät an, wenn eine gesperrte Operation auftritt.
    - **Startmenü-Shortcut in der Gruppe LANDesk Management anzeigen:** Zeigt ein Programmsymbol für den Endpunktsicherheit-Client im Startmenü an (**Start > Programme > LANDesk Management**).
- **Globale Hotkeys:** Gibt die Hotkey-Shortcuts an, die für bestimmte Endpunktsicherheitsfunktionen verwendet werden.
    - **Hotkey zur Umgehung der Gerätesteuerung:** Hier können Sie eine Hotkey-Sequenz definieren, mit der Systemadministratoren temporär Zugriff auf ein blockiertes Gerät erhalten. Sie können den Standard-Hotkey (Strg + Umschalt + Nach oben) ändern. Um die gewünschte Hotkey-Sequenz einzugeben, setzen Sie den Cursor in das Textfeld und drücken (und halten) die Tasten in der gewünschten Reihenfolge.
- **Als Standard festlegen:** Weist diesen Einstellungen als die Standardeinstellungen für Tasks zu, die Endpunktsicherheit verwenden.
- **Speichern:** Speichert die Änderungen und schließt das Dialogfeld.

Informationen zur Endpunktsicherheit: Seite "Digitale Signaturen"

Diese Seite verwenden Sie zum Anzeigen und Verwalten von Listen vertrauenswürdiger Dateien. Listen der vertrauenswürdigen Dateien umfassen Dateien, die mit einem bestimmten Satz von Rechten (Berechtigungen oder Autorisierungen) konfiguriert wurden, die die Ausführung bestimmter Aktionen für diese Datei *durch* eine Anwendung zulässt oder verweigert.

Diese Seite enthält folgende Optionen:

- **Listen der vertrauenswürdigen Dateien:** Zeigt die Dateilisten, die Dateien mit für HIPS konfigurierte Rechte aufweisen.
    - **Hinzufügen:** Öffnet das Dialogfeld **Listen der vertrauenswürdigen Dateien konfigurieren**, in dem Sie Ihre Listen der vertrauenswürdigen Dateien verwalten können.
    - **Bearbeiten:** Hiermit können Sie die Liste der vertrauenswürdigen Dateien bearbeiten.
    - **Entfernen:** Hiermit können Sie die Liste der vertrauenswürdigen Dateien entfernen.

- **Optionen für Erfassungsaktivität:** Gibt an, wie Dateiaktivität behandelt wird, wenn der Schutzmodus auf Erfassung eingestellt ist.
    - **Erfassungsliste:** Zeigt die Liste der vertrauenswürdigen Dateien an, auf die die erfasste Dateiaktivität angewendet wird.
    - **Erfassungsaktivität nur zur Erfassungsliste hinzufügen:** Beschränkt die erfasste Dateiaktivität auf die angegebene Dateiliste.
    - **Erfassungsaktivität zu jeder Liste hinzufügen, in der dieselbe Datei bereits enthalten ist:** Die erfasste Dateiaktivität kann auf jede Dateiliste angewendet werden, die diese Datei enthält.

Informationen zur Endpunktsicherheit: Standardrichtlinie

Diese Seite verwenden Sie, um Sicherheitsrichtlinien für Geräte innerhalb des vertrauenswürdigen Netzwerks und Richtlinien für Geräte außerhalb des vertrauenswürdigen Netzwerks zu konfigurieren.

- **Innerhalb des vertrauenswürdigen Speicherorts:** Gibt die Komponenteneinstellungen an, die auf Geräte angewendet werden, wenn diese mit einem vertrauenswürdigen Speicherort verbunden sind.
- **Außerhalb des vertrauenswürdigen Speicherorts:** Gibt die Komponenteneinstellungen an, die auf Geräte angewendet werden, wenn diese mit einem vertrauenswürdigen Speicherort verbunden sind.

Informationen zur Endpunktsicherheit: Seite "Standortrichtlinien"

Diese Seite verwenden Sie zum Definieren der vertrauenswürdigen Speicherorte. Ein vertrauenswürdiger Speicherort besteht aus einer Sammlung von Netzwerkadressen nach IP-Adresse, IP-Bereich oder Subnetz.

Diese Seite enthält folgende Optionen:

- **Standorterkennung verwenden (Richtlinien für mehrere Standorte einrichten):**
    - **Hinzufügen:** Klicken Sie, um eine neue Erkennungsrichtlinie für einen vertrauenswürdigen Standort hinzuzufügen.
    - **Bearbeiten:** Gibt Ihnen die Möglichkeit, den ausgewählten vorhandenen vertrauenswürdigen Speicherort zu ändern.
    - **Entfernen:** Entfernt den ausgewählten vertrauenswürdigen Speicherort.

HINWEIS: Standardrichtlinie
Die Standardrichtlinie wird angewendet, wenn ein Gerät mit keinem der aufgeführten Standorte verknüpft ist.

Informationen zum Dialogfeld "Speicherort hinzufügen"

Dieses Dialogfeld verwenden Sie zum Erstellen eines neuen Speicherorts für Ihre Richtlinien zur Erkennung von vertrauenswürdigen Speicherorten. Sie können eine IP-Adresse, einen IP-Bereich oder eine Subnetzadresse eingeben.

Dieses Dialogfeld enthält folgende Optionen:

- **Name:**
- **Bedingungen:**
  - **Typ:**
  - **Wert:**
  - **Hinzufügen:**
  - **Bearbeiten:**
  - **Löschen:**
  - **Importieren:**
- **Coreserver:**
  - **Überprüfen, ob Coreserver im Netzwerk existiert:** Wählen Sie diese Option aus, um sicherzustellen, dass der Coreserver in einem Netzwerk läuft, bevor einem Gerät der Verbindungsaufbau mit dem betreffenden Netzwerk ermöglicht wird. Ein Bereich von IP-Adressen wird manchmal von mehr als einem Netzwerk verwendet. Diese Option bietet zusätzliche Sicherheit, indem sie den Netzwerkzugriff beschränkt. Wird auf dem Netzwerk, auf das zugegriffen wird, kein Coreserver gefunden, so wird die Verbindung deaktiviert. (Hinweis: Aktivieren Sie diese Option nicht, wenn Sie sich sicher sind, dass die in der Zugriffsliste geführten Netzwerkadressen vertrauenswürdig sind, oder wenn Sie es bevorzugen, den Datenverkehr im Netzwerk dadurch zu reduzieren, dass keine Pings an den Coreserver gesendet werden.
  - **Hinzufügen:** Gibt Ihnen die Möglichkeit, einen Coreserver zur Liste hinzuzufügen.
  - **Entfernen:** Entfernt den ausgewählten Coreserver.
- **OK:**
- **Abbrechen:**

Verwandte Themen:

Host Intrusion Prevention System (HIPS) – Übersicht

HIPS steht für "Host-based Intrusion Prevention System". HIPS bietet eine zusätzliche Sicherheitsebene über Patch Management, Antivirus, Anti-Spyware und der Firewallkonfiguration hinaus, die bösartige Übergriffe auf Ihre verwalteten Geräten verhindert. HIPS überwacht kontinuierlich spezifizierte Prozesse, Dateien, Anwendungen und Registrierungsschlüssel, um nicht autorisierte Aktionen zu verhindern. Sie entscheiden selbst, welche Anwendungen auf welche Weise auf Geräten ausgeführt werden dürfen.

Da es sich nicht um ein definitionsbasiertes, sondern ein regelbasiertes (d. h. signaturbasiertes) System handelt, kann HIPS Systeme effektiver vor Zero-Day-Angriffen (Missbrauch von anfälligem Code, bevor diese Sicherheitslücken erkannt und definiert werden und Patches zur Verfügung stehen) schützen.

Im Unterschied zur Erkennung und Reparatur von Anfälligkeiten, zur Erkennung und Entfernung von Spyware oder Antivirusscans und Quarantänemaßnahmen erfordert der HIPS-Schutz keine ständigen Dateiupdates (Patchdateien, Definitions-/Musterdateien oder Signaturdatenbankdateien).

HIPS schützt Server und Arbeitsstationen, indem Softwareagenten zwischen Anwendungen und dem Kernel des Betriebssystems platziert werden. Unter Verwendung vordefinierter Regeln, die auf dem typischen Verhalten von Malware-Angriffen basieren, analysieren diese Systeme Aktivitäten wie Netzwerkverbindungsanforderungen, Lese- oder Schreibversuche im Speicher oder Zugriffsversuche auf bestimmte Anwendungen. Ordnungsgemäßes Verhalten wird zugelassen, während destruktives Verhalten blockiert sowie verdächtiges Verhalten für die weitere Auswertung gekennzeichnet wird.

Der Zugriff auf das Extra "HIPS" und die zugehörigen Funktionen erfolgt von der Hauptkonsole aus (**Extras > Sicherheit und Compliance > Agenteneinstellungen**). Mit dem Extra "HIPS" können Sie Installations-, Aktualisierungs- und Entfernungstasks für den HIPS-Agenten erstellen sowie HIPS-Einstellungen konfigurieren, die auf Zielgeräten, die Sie schützen möchten, bereitgestellt werden können. Darüber hinaus können Sie HIPS-Anzeige/-Interaktionseinstellungen anpassen. Mit diesen Einstellungen wird festgelegt, wie HIPS auf verwalteten Geräten angezeigt wird und arbeitet und welche interaktiven Optionen den Endbenutzern zur Verfügung stehen. Des Weiteren können Sie HIPS-Aktivitäts- und Statusinformationen für geschützte Geräte anzeigen.

Eine Komponente der Endpunktsicherheit

HIPS ist eine Komponente der umfassenden Lösung "Endpunktsicherheit", zu der auch die Extras "Standorterkennung (Netzwerkverbindungssteuerung)", "LANDesk Firewall" und "Gerätesteuerung" gehören.

Proaktive Sicherheit

HIPS sorgt wie folgt proaktiv für die Sicherheit Ihrer verwalteten Geräte:

- Schutz auf der Kernel-Ebene vor Anwendungen, die darauf abzielen, Änderungen an den Binarys (oder an jeder anderen von Ihnen angegebenen Datei) auf Ihrem Computer vorzunehmen oder den Programmspeicher laufender Prozesse zu ändern. Änderungen in bestimmten Abschnitten der Registrierung werden blockiert und Rootkit-Prozesse werden aufgedeckt.
- Einsatz von Speicherschutz gegen Pufferüberlauf und Heap-Exploits.
- Implementierung von Schutzplänen, die Angreifer daran hindern, Code in Datensegmenten zu erstellen und auszuführen.
- Überwachung der Systeme auf nicht autorisierten oder ungewöhnlichen Dateizugriff.
- Echtzeitschutz für Ihren Computer, ohne auf Signaturdatenbanken angewiesen zu sein.

Sicherheit auf Systemebene

HIPS bietet folgende Systemsicherheitsfunktionen:

- Regelbasierter Dateisystemschutz auf Kernel-Ebene
- Registrierungsschutz
- Startkontrolle
- Erkennung maskierter Rootkits
- Netzwerkfilter
- Prozess- sowie Datei-/Anwendungszertifizierung
- Dateischutzregeln, die Aktionen beschränken, die Ausführungsprogramme auf bestimmten Dateien ausführen können

HIPS-Konsolenfunktionen

Mit HIPS können Administratoren separate Profile für unterschiedliche Benutzergruppen über HIPS-Einstellungen definieren und verwalten. HIPS-Einstellungen erfüllen die Anforderungen aller Benutzergruppen, indem sie Administratoren die Möglichkeit bieten, mehrere, hochgradig flexible Konfigurationen für unterschiedliche Benutzerprofile zu erstellen.

Alle HIPS-Einstellungen können benutzerdefinierten Kennwortschutz, WinTrust-Handling, Schutzmodus, benutzerdefinierte Positivlisten, NAC- und Anwendungszugriffssteuerungsrichtlinien, Dateizertifizierungen und Dateischutzregeln umfassen.

HIPS-Clientfunktionen

Mit dem leistungsstarken HIPS-Client (der für verwaltete Geräte bereitgestellt wird) können Administratoren steuern, welche Anwendungen auf welche Weise auf den Desktops und Servern des Unternehmens ausgeführt werden dürfen.

Die HIPS-Clientsoftware arbeitet mit bewährten Heuristik- und Verhaltenserkennungstechniken, die es ermöglichen, typische Muster und Aktionen destruktiver Programme (Code) aufzudecken. Beispiel: Eine Datei, die den Versuch unternimmt, in die Systemregistrierung zu schreiben, könnte blockiert und als potenziell bösartig gekennzeichnet werden. Der HIPS-Client nutzt eine Vielzahl proprietärer Techniken, die eine zuverlässige Erkennung von Malware ermöglichen, noch bevor eine Signatur identifiziert wird.

Unterstützte Geräteplattformen

Aktuelle Informationen zu den Clientplattformen, die Unterstützung für HIPS bieten, finden Sie im Dokument "OS Compatibility Feature Matrix" auf der Website der LANDesk Benutzercommunity:

LANDesk Benutzercommunity – Startseite

WICHTIG: HIPS wird weder auf Coreservern noch auf Rollup-Cores unterstützt
HIPS sollte weder auf einem Coreserver noch auf einem Rollup-Core installiert oder bereitgestellt werden. Sie können HIPS jedoch auf einer zusätzlichen Konsole bereitstellen.

Unterstützte Antivirusprodukte

HIPS ist sowohl mit der LANDesk Security Suite Antiviruslösung als auch mit mehreren Antivirusprodukten von Drittanbietern kompatibel. Kompatibilität bedeutet, dass Antivirusprozesse wie Scans, Echtzeitschutz etc. durch HIPS nicht beeinträchtigt werden.

Stellen Sie sicher, dass auf den verwalteten Geräten, die Sie mit HIPS konfigurieren möchten, eines der folgenden Produkte installiert ist:

- LANDesk Antivirus
- Symantec Antivirus (Versionen 7, 8, 9, 10.1, 10.2)
- McAfee VirusScan (Versionen 7.0, 8.0, 8.5i)
- Trend Micro PC-cillin (Versionen 2005, 2006)
- Trend Micro OfficeScan (Versionen 6.5, 7.3)
- Trend Micro ServerProtect (Versionen 5.58)
- CA eTrust InoculateIT (Version 6.0)

- CA eTrust Antivirus (Versionen 7.0, 7.1, 8.0, 8.1)
- ESET NOD32 (Version 2.7)

HIPS darf KEINESFALLS auf Geräten bereitgestellt werden, auf denen irgendein anderes Antivirus-Produkt installiert ist.

HIPS-Lizenzierung

Für den Zugriff auf das Extra "HIPS" müssen Sie zunächst Ihren Coreserver mit einer HIPS-Lizenz aktivieren.

Informationen zur HIPS-Lizenzierung erhalten Sie von Ihrem Händler oder auf der LANDesk Website.

LANDesk Startseite

Rollenbasierte Administration mit HIPS

HIPS verwendet, wie Patch und Compliance, die rollenbasierte Administration, um den Benutzerzugriff auf Funktionen zu regeln. Die rollenbasierte Administration ist das Zugriffs- und Sicherheitsmodell, mit dem LANDesk Administratoren den Zugriff der Benutzer auf Extras und Geräte steuern. Jedem Benutzer werden bestimmte Rollen und Bereiche zugewiesen, die festlegen, mit welchen Funktionen dieser Benutzer arbeiten und welche Geräte er verwalten kann.

Der Administrator weist anderen Benutzern diese Rollen mithilfe des Extras "Benutzer" in der Konsole zu. HIPS ist im Recht "Agenteneinstellungen" enthalten, das im Dialogfeld "Rollen" unter der Rechtegruppe "Sicherheit" erscheint. Damit ein Benutzer HIPS-Funktionen anzeigen und verwenden kann, müssen ihm die hierfür erforderlichen Zugriffsrechte für Agenteneinstellungen erteilt werden.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Agenteneinstellungen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Mit dem Recht "Agenteneinstellungen" können Benutzer Folgendes tun:

- die Host Intrusion Prevention System (HIPS)-Funktionen im Menü "Extras" und in der Toolbox der Konsole anzeigen und öffnen,
- verwaltete Geräte für den HIPS-Schutz konfigurieren,
- HIPS-Einstellungen verwalten (Kennwortschutz, signiertes Code-Handling, Aktion, Schutzmodus, Dateizertifizierungen, Dateischutzregeln u.s.w.),
- HIPS-Installationstasks/-Aktualisierungstasks und Einstellungsänderungs-Tasks bereitstellen,
- HIPS-Aktivität für geschützte Geräte anzeigen,
- HIPS-Datengrenzwerteinstellungen zur Aufzeichnung und Darstellung von HIPS-Aktivitäten definieren.

HIPS – Wesentliche Tasks im Überblick

Die nachstehende Liste gibt einen Überblick über die wesentlichen Tasks zur Konfiguration, Implementierung und Verwendung von des HIPS-Schutzes. Die funktionsspezifischen Hilfethemen liefern detaillierte Informationen zu den Konzepten, Verfahren und Prozessen.

- Konfiguration verwalteter Geräte für HIPS-Schutz (d. h. Bereitstellung des Agenten auf Zielgeräten)
- Konfiguration von HIPS-Optionen mit HIPS-Einstellungen, wie z. B. signiertes Codehandling, Schutzmodus, Positivlisten (Anwendungen, die auf Geräten ausgeführt werden dürfen), Dateizertifizierung, Dateischutzregeln und Endbenutzer-Interaktivität/Optionen
- Erkennen von Datei- und Anwendungsverhalten auf Geräten mit dem HIPS-Erfassungsmodus
- Durchsetzen des HIPS-Schutzes auf verwalteten Geräten mit dem automatischen HIPS-Blockiermodus
- HIPS-Aktivität für geschützte Geräte anzeigen

Konfigurieren von Geräten für HIPS-Schutz

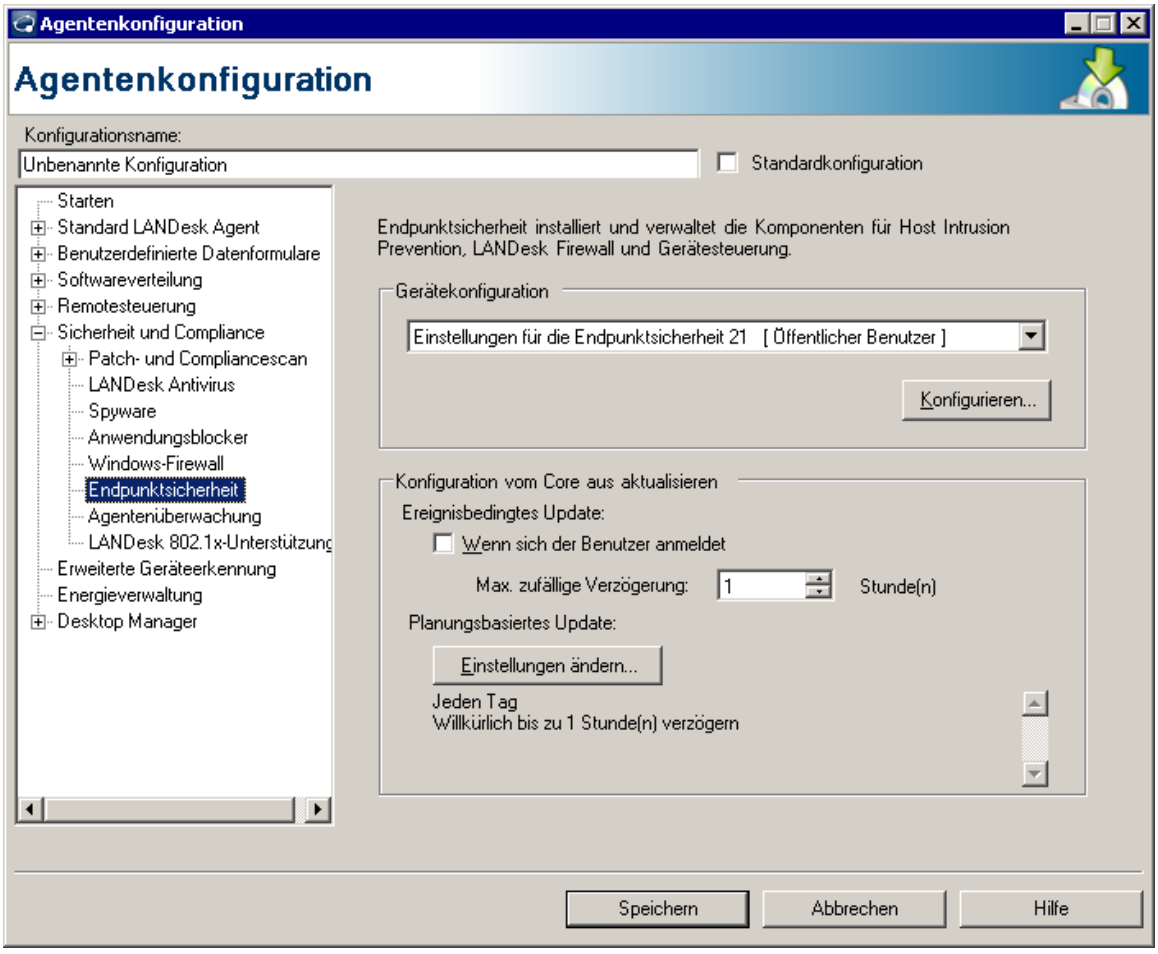
Damit verwaltete Geräte vor Zero-Day-Angriffen geschützt werden können, muss der Agent für Endpunktsicherheit auf dem Gerät installiert werden. Der Agent für Endpunktsicherheit stellt einen separaten Agentendienst dar, der alle Komponenten der Endpunktsicherheit, einschließlich HIPS, verwaltet.

Sie können Geräte entweder bei der ursprünglichen Agentenkonfiguration für das Gerät oder im Rahmen eines separaten Installations- oder Updatetasks für HIPS konfigurieren.

So installieren oder aktualisieren Sie HIPS mithilfe einer Agentenkonfiguration auf verwalteten Geräten

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie in der Symbolleistenschaltfläche auf **Neues Windows**.
3. Wenn Sie die gewünschten Einstellungen für die Agentenkonfiguration eingegeben haben, müssen Sie zuerst auf die **Startseite** klicken und unter **Sicherheit** die Option **Endpunktsicherheit** auswählen. (Damit wird der Agent für die Zielgeräte bereitgestellt, aber Sie müssen noch HIPS-Einstellungen auswählen.)

4. Jetzt erhalten Sie Zugriff auf die Optionen der Seite **Endpunktsicherheit**.

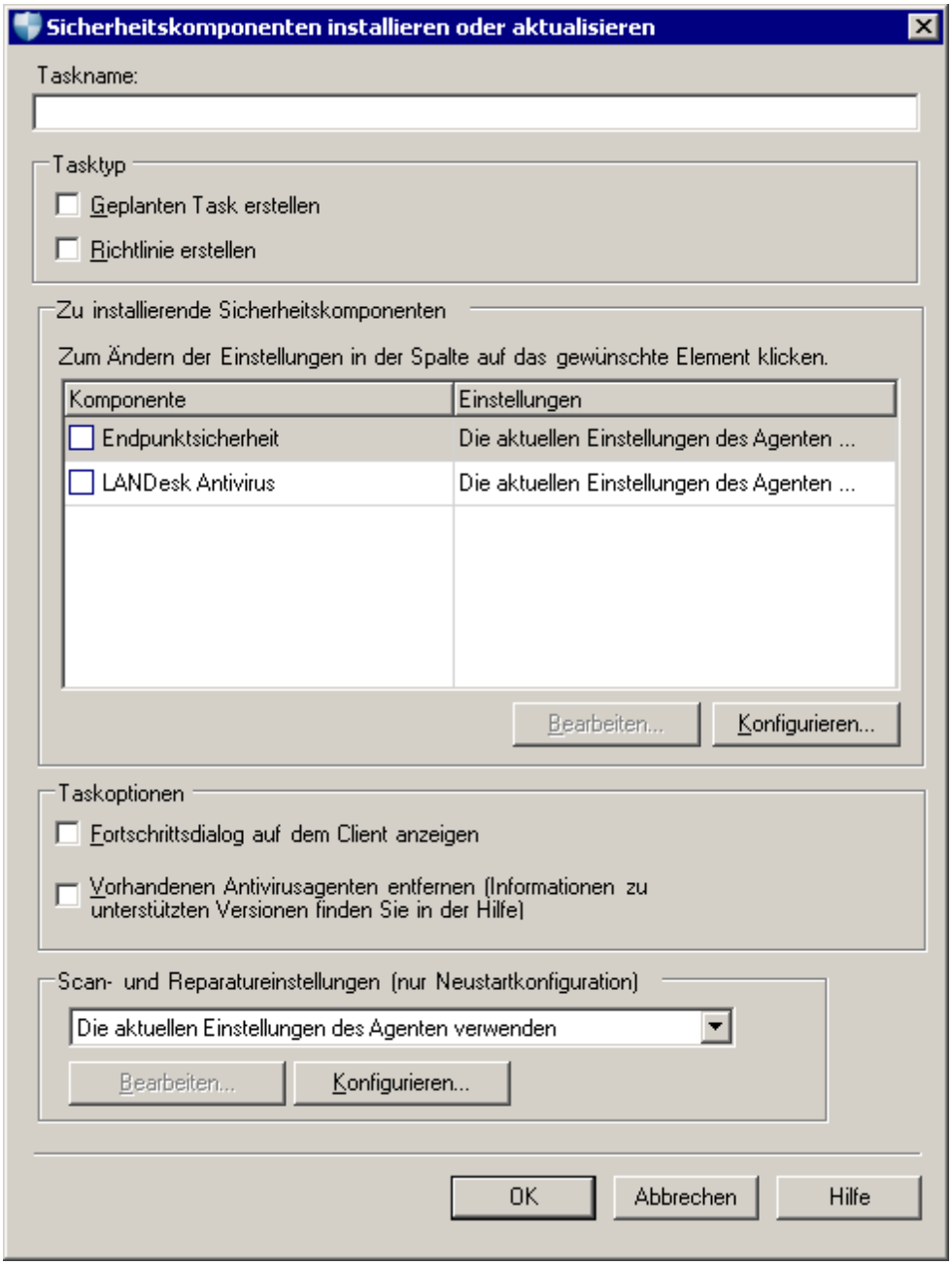


5. Wählen Sie eine der Einstellungen aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Die Einstellungen für die Endpunktsicherheit enthalten (neben Einstellungen für andere Sicherheitskomponenten) Einstellungen für HIPS. Die HIPS-Einstellungen legen Folgendes fest: ob der HIPS-Client kennwortgeschützt ist, WinTrust signiertes Code-Handling eingestellt ist, Aktionen auf Programme, die beim Systemstart hinzugefügt werden, sowie Pufferüberlaufschutz, Betriebsmodus, Positivlisten, Dateizertifikate und Dateischutzregeln.
6. Legen Sie alle gewünschten Einstellungen für die Agentenkonfiguration fest und klicken Sie dann auf **Speichern**.

Wenn Sie HIPS zu einem späteren Zeitpunkt installieren oder aktualisieren möchten, können Sie dies mithilfe eines separaten Task über das Extra **Agenteneinstellungen** in der Konsole tun.

So wird HIPS als separater Task installiert oder aktualisiert

1. Klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Agenteneinstellungen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten installieren/aktualisieren**.



3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.

5. Wählen Sie eine der Einstellungen für die Endpunktsicherheit aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Die Einstellungen für die Endpunktsicherheit enthalten (neben Einstellungen für andere Sicherheitskomponenten) Einstellungen für HIPS.
6. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster von Zielgeräten anzeigen möchten, wählen Sie die Option **Fortschrittsdialog auf dem Client anzeigen** aus.
7. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste aus, um deren Neustartkonfiguration (Option "Nur Neustartkonfiguration") auf die Agentenkonfiguration anzuwenden, die Sie erstellen möchten. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Denken Sie daran, dass *nur diejenigen Neustartoptionen*, die Sie unter den von Ihnen ausgewählten Scan- und Reparatureinstellungen angegeben haben, von der Agentenkonfiguration dieser Endpunktsicherheit-Agentenbereitstellung auf Zielgeräten verwendet werden. Sie können eine vorhandene Scan- und Reparatureinstellung verwenden, die bereits die gewünschte Neustartkonfiguration beinhalten, oder Sie können eine komplett neue Scan- und Reparatureinstellung speziell für Ihre Agentenbereitstellung erstellen.
8. Klicken Sie auf **OK**.

Entfernen von HIPS auf Geräten

Wenn Sie HIPS von verwalteten Geräten entfernen möchten, können Sie hierfür auch einen separaten Task in der Konsole verwenden.

So entfernen Sie HIPS

1. Klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Agenteneinstellungen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten entfernen**.
3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.
5. Wählen Sie die Komponente "Endpunktsicherheit" aus, um diesen Agenten zu entfernen, der HIPS enthält.
6. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster von Zielgeräten anzeigen möchten, wählen Sie die Option **Fortschrittsdialog auf dem Client anzeigen** aus.
7. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste der verfügbaren Einstellungen aus, um deren Neustartkonfiguration auf den Task anzuwenden, die Sie gerade erstellen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Der Task verwendet *nur* die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten beim Entfernen des Agenten.
8. Klicken Sie auf **OK**.

Anpassen des HIPS-Schutzes über HIPS-Einstellungen

Mit den HIPS-Einstellungen haben Sie vollständige Kontrolle darüber, wie HIPS auf Zielgeräten arbeitet und darüber, welche Optionen dem Endbenutzer zur Verfügung stehen.

Dieser Abschnitt beschreibt, wie HIPS-Einstellungen erstellt und verwaltet werden.

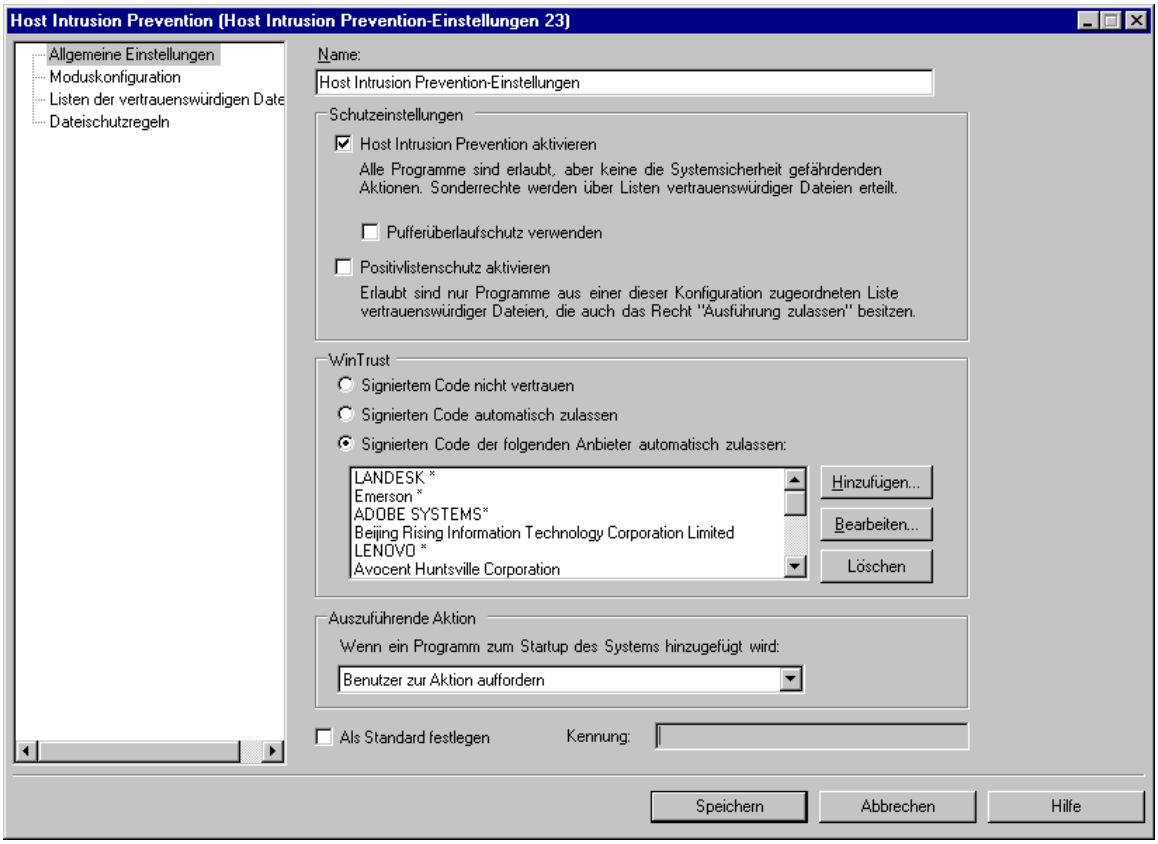
- "Erstellen von HIPS-Einstellungen" auf Seite 727
- "Ändern der HIPS-Standardeinstellungen" auf Seite 728
- "Anzeigen von HIPS-Einstellungen eines Geräts im Inventar" auf Seite 728
- "Hilfe zu HIPS" auf Seite 730

Erstellen von HIPS-Einstellungen

Sie können HIPS-Einstellungen für eine HIPS-Installation oder einen Aktualisierungstask oder einen Einstellungsänderungstask erstellen und anwenden. Sie können beliebig viele HIPS-Einstellungen erstellen. HIPS-Einstellungen können für einen bestimmten Zweck, Zeitpunkt oder Satz von Zielgeräten definiert werden.

So definieren Sie HIPS-Einstellungen

1. Klicken Sie im Fenster des Extras **Agenteneinstellungen** mit der rechten Maustaste auf **Host Intrusion Prevention-System** und klicken Sie dann auf **Neu**.



2. Geben Sie auf der Seite **Allgemeine Einstellungen** einen Namen für die HIPS-Einstellungen ein und geben Sie dann die allgemeinen Anforderungen und Aktionen an. Wenn Sie Informationen zu einer Option benötigen, klicken Sie auf "Hilfe zu HIPS" auf Seite 730.

3. Auf der Seite **Moduskonfiguration** wählen Sie aus, ob Sie den automatischen HIPS-Sperrschutzmodus oder den Erfassungsmodus durchsetzen möchten. Sie können auch auf der Basis der derzeit zertifizierten Dateien eine Positivliste (mit zulässigen Anwendungen zur Ausführung auf Geräten) erstellen und angeben, ob die Generierung der Positivliste zunächst für eine gewisse Zeitspanne ausgeführt werden soll und anschließend der automatische Sperrmodus neu durchgesetzt werden soll oder ob Sie den Erfassungsmodus weiter verwenden möchten. (**HINWEIS:** Wenn Sie den Erfassungsmodus als allgemeinen Schutzmodus wählen und eine Positivliste erstellen möchten, ist die Option zum Durchsetzen des automatischen Sperrmodus deaktiviert.
4. Öffnen Sie die Seite **Listen der vertrauenswürdigen Dateien**, um Listen vertrauenswürdiger Dateien hinzuzufügen, zu ändern oder zu löschen.
5. Öffnen Sie die Seite **Dateischutzregeln**, um Dateischutzregeln hinzuzufügen, zu ändern, zu priorisieren oder zu löschen. HIPS enthält eine vordefinierten (Standard) Schutzregelsatz.
6. Sie können jederzeit auf einer beliebigen Einstellungsseite auf **Speichern** klicken, um Ihre konfigurierten Optionen für die HIPS-Einstellung zu speichern oder auf **Abbrechen**, um das Dialogfeld ohne Speichern der Einstellungen zu verlassen.

Nachdem Sie die HIPS-Einstellungen konfiguriert haben, können Sie diese über einen Installation- oder Updatetask oder mithilfe eines Tasks zum Ändern von Einstellungen auf Zielgeräte übertragen.

Ändern der HIPS-Standardeinstellungen

Die HIPS-Standardeinstellungen der Geräte werden als Teil der ursprünglichen Agentenkonfiguration bereitgestellt. Es kann zu einem späteren Zeitpunkt sinnvoll sein, diese HIPS-Standardeinstellungen auf bestimmten Geräten zu ändern. HIPS bietet eine Möglichkeit, diese Änderung vorzunehmen, ohne erneut eine komplett neue und vollständige Agentenkonfiguration bereitstellen zu müssen.

Verwenden Sie hierfür den Task **Einstellungen ändern** in der Dropdownliste der Symbolleistenschaltfläche **Task erstellen**. In das eingeblendete Dialogfeld können Sie einen eindeutigen Namen für den Task eingeben, festlegen, ob es sich um einen geplanten Task oder eine Richtlinie handelt, und entweder vorhandene HIPS-Einstellungen als Standard auswählen oder mithilfe der Schaltfläche **Bearbeiten** neue HIPS-Einstellungen als Standard für Zielgeräte erstellen.

Anzeigen von HIPS-Einstellungen eines Geräts im Inventar

Sie können HIPS-Einstellungen in der Inventaransicht eines Geräts aufdecken und/oder überprüfen.

Klicken Sie hierzu mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie dann auf **Inventar > LANDesk Management > Host Intrusion Prevention-System**.

Zusammenführen von HIPS-Zertifizierungen

Sie können HIPS-zertifizierte Dateien aus einer HIPS-Einstellung in eine oder mehrere andere HIPS-Einstellungen überführen. Auf diese Weise können Einstellungen für zertifizierte Dateien schnell und einfach aktualisiert und freigegeben werden.

So führen Sie HIPS-zertifizierte Dateien zusammen

1. Klicken Sie im Fenster des Extras **Agenteneinstellungen** mit der rechten Maustaste auf **Host Intrusion Prevention-System** und klicken Sie dann auf **Zertifizierte Dateien zusammenführen**.
2. Wählen Sie eine Quellkonfiguration aus der Liste aus.

3. Wählen Sie, ob Sie Unterschiede in den zertifizierten Dateien zusammenführen oder alle zertifizierten Dateien einfach ersetzen möchten.
4. Wählen Sie die Zielkonfigurationen aus.
5. Klicken Sie auf **OK**.

Hilfe zum Zusammenführen von HIPS-Zertifizierungen

Informationen zum Dialogfeld "Zertifizierte Dateien zusammenführen"

Dieses Dialogfeld verwenden Sie, um eine Zusammenführung von zertifizierten HIPS-Dateien zwischen ein oder mehreren HIPS-Einstellungen zu konfigurieren und auszuführen.

Dieses Dialogfeld enthält folgende Optionen:

- **Quellkonfiguration:** Gibt die HIPS-Einstellungen an, deren zertifizierte Dateien Sie mit den gewählten Zielkonfigurationen zusammenführen möchten.
- **Unterschiede in zertifizierten Dateien zusammenführen:** Ersetzt alle gemeinsamen zertifizierten Dateien in den Zielkonfigurationen mit jenen in der Quellkonfiguration und fügt eindeutige zertifizierte Dateien aus der Quellkonfiguration zur den Zielkonfigurationen hinzu.
- **Zertifizierte Dateien ersetzen:** Setzt durch, dass die zertifizierten Dateien in der Quellkonfiguration alle Dateien in den Zielkonfigurationen ersetzen.
- **Zielkonfigurationen:** Gibt die Zielkonfigurationen an, die mit der Quellkonfiguration zusammengeführt werden sollen. Wählen Sie Ziele aus der Liste der verfügbaren Konfigurationen aus.

Grundlegendes zum HIPS-Erfassungsmodus

HIPS kann in einem der folgenden Schutzmodi ausgeführt werden: Automatisch, Erfassen, Nur protokollieren oder Verweigern.

Verwendung des HIPS-Erfassungsmodus

Nachstehend finden Sie eine Beschreibung des HIPS-Erfassungsmodus:

- Im Erfassungsmodus "lernt" HIPS, welche Arten von Anwendungen auf dem Gerät installiert sind, wie sie sich verhalten und welche Rechte (Privilegien) sie besitzen.
- HIPS überwacht die Aktivitäten auf dem Gerät und zeichnet Informationen in einem Aktionsprotokoll auf.
- Diese Aktionsverlaufsdaten werden vom Gerät an den Coreserver weitergeleitet.
- Administratoren lesen den Aktionsverlauf, um herauszufinden, welche Anwendungen welche Aktionen auf dem Gerät ausführen. (Die Dateien/Anwendungen und zugehörigen Rechte, die in der Aktionsverlaufsdatei (XML-Format) gelistet sind, werden auf der Seite "Dateizertifizierungen" des Dialogfelds für die HIPS-Einstellungen angezeigt.)
- Administratoren können die HIPS-Einstellungen so ändern, dass sie Privilegien für relevante Anwendungen zulassen oder ablehnen.

Der Erfassungsmodus kann auf verwalteten Geräten angewendet werden und lässt im Allgemeinen ein Auftreten von HIPS-Übertretungen zu, bis eine neue HIPS-Einstellung bereitgestellt wird. Er kann auch zu Anfang für eine bestimmte Zeit angewendet werden, damit erkannt wird, welche Anwendungen ausgeführt werden, welches Verhalten diese zeigen und damit eine Positivliste (mit den zulässigen Anwendungen zur Ausführung auf Geräten) erstellt werden kann. Wenn der allgemeine Schutzmodus "automatisch sperren" ist, können Sie dennoch den Erfassungsmodus zur Erkennung des Anwendungsverhaltens verwenden und dann den automatischen Sperrmodus wieder durchsetzen, sobald die Erfassungsperiode abgelaufen ist.

WICHTIG: Beachten Sie, dass sowohl der Coreserver als auch das verwaltete Gerät im Erfassungsmodus betrieben werden müssen, damit die Aktionsverlaufskommunikation stattfinden kann.

Hilfe zu HIPS

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten einer HIPS-Einstellung (Konfigurationsdatei). Beim Erstellen von HIPS-Einstellungen definieren Sie zuerst die allgemeinen Anforderungen und Aktionen und fügen dann spezifische Dateizertifizierungen hinzu. Sie können beliebig viele HIPS-Einstellungen erstellen und jederzeit bearbeiten.

Wenn Sie die HIPS-Standardeinstellungen des Geräts ändern möchten, ohne den HIPS-Agenten erneut zu installieren oder erneut eine vollständige Agentenkonfiguration bereitzustellen, sollten Sie die von Ihnen gewünschten Änderungen für Optionen im Dialogfeld "HIPS-Einstellungen" vornehmen, die neuen Einstellungen einem Einstellungsänderungs-Task zuordnen und diesen Einstellungsänderungs-Task dann auf Zielgeräten bereitstellen.

Dieses Dialogfeld umfasst die folgende Seiten:

- "Informationen zum Dialogfeld "HIPS: Allgemeine Einstellungen"" auf Seite 730
- "Informationen zum Dialogfeld "HIPS: Moduskonfiguration"" auf Seite 732
- "Informationen zum Dialogfeld "HIPS: Dateischutzregeln"" auf Seite 733
- "Informationen zum Dialogfeld "HIPS: Dateischutzregel konfigurieren"" auf Seite 733

Informationen zum Dialogfeld "HIPS: Allgemeine Einstellungen"

Diese Seite verwenden Sie zum Konfigurieren der allgemeinen Schutzeinstellungen und Aktionen für HIPS.

Diese Seite enthält folgende Optionen:

- **Name:** Kennzeichnet die HIPS-Einstellungen mit einem eindeutigen Namen. Dieser Name wird in der Liste der HIPS-Einstellungen in einem Dialogfeld "Sicherheitskomponenten installieren oder aktualisieren" angezeigt.

- **Schutzeinstellungen:** Es gibt zwei Schutztypen: HIPS und Positivliste. Sie können einen von beiden oder beide auswählen. Beide Schutztypen verwenden dieselbe Betriebsart, nämlich diejenige, die auf der Seite "Moduskonfiguration" ausgewählt wurde. (**HINWEIS:** Eine Ausnahme gibt es hinsichtlich der Durchsetzung dieses allgemeinen Schutzes. Wenn Sie den Schutzmodus "Erfassen" angeben und die Option "Nur Positivliste zum Erfassen ("Lernen") verwenden" markiert haben, werden *nur* Anwendungen auf der Positivliste erfasst und der HIPS-Schutz wird auf den Modus für automatisches Blockieren gesetzt.
    - **Host Intrusion Prevention aktivieren:** Schaltet den HIPS-Schutz ein. Alle Programme dürfen ausgeführt werden (es sei denn, der Einsatz eines Programms gefährdet die Systemsicherheit), wie in den vordefinierter Schutzregeln festgelegt. Sie können Programmdateien über Listen vertrauenswürdiger Dateien besondere Rechte einräumen, indem Sie benutzerdefinierte Dateizertifizierungen konfigurieren. Der HIPS-Schutz beobachtet das Anwendungsverhalten (ob die Anwendung andere ausführbare Dateien ändern darf, die Registrierung verändern darf usw.) und setzt Sicherheitsregeln durch.
        - **Pufferüberlaufschutz verwenden:** Damit werden Geräte vor Systemspeicherexploits geschützt, die Programme oder Prozesse ausnutzen, die auf eine Benutzereingabe warten.

          HINWEIS: Pufferüberlaufschutz (BOP: Buffer Overflow Protection) kann auf 32-Bit-Windows-Geräten unabhängig davon aktiviert werden, ob der Prozessor NX/XD (No eXecute/eXecute Disable)-Unterstützung bietet. Wenn der Prozessor keine NX/XD-Unterstützung bietet, so wird diese emuliert. Wenn der Prozessor zwar NX/XD-Unterstützung bietet, diese jedoch entweder im BIOS oder in der Bootkonfiguration abgeschaltet ist, dann kann BOP nicht aktiviert werden. Beachten Sie, dass der Endpunktsicherheits-Client unabhängig davon angezeigt wird, ob BOP auf dem Endbenutzergerät aktiviert oder deaktiviert ist. BOP wird auf 64-Bit-Windows-Geräten nicht unterstützt, da die Funktion "Kernel Patch Protection" (KPP) ein Patchen des Kernels verhindert.

          WICHTIG: Wir empfehlen Ihnen dringend, den Pufferüberlaufschutz (BOP) zunächst auf Ihren spezifischen Hardwarekonfigurationen zu testen, bevor Sie eine groß angelegte Bereitstellung für die verwalteten Geräte in Ihrem Netzwerk vornehmen. Manche Konfigurationen mit älteren Prozessoren (vor Pentium 4 mit HT oder HyperThreading) und bestimmten Windows-Betriebssystemversionen bieten unter Umständen keine volle Unterstützung für Pufferüberlaufschutz.

    - **Positivlistenschutz aktivieren:** Schaltet den Positivlistenschutz ein. Dies bedeutet, dass nur solche Anwendungen ausgeführt werden dürfen, die in der Liste der vertrauenswürdigen Dateien aufgeführt sind und bei denen in der Dateizertifizierung die Option "Ausführung zulassen" aktiviert ist.
        - **Verhindern, dass Windows Explorer ausführbaren Dateien ändert oder löscht:** Aktivieren Sie diese Option, wenn Sie nicht möchten, dass Windows ausführbare Dateien ändert oder löscht.
- **Auszuführende Aktion:** Bestimmt die Aktion, die beim Hinzufügen eines Programms zum Startordner des Geräts ausgeführt wird. Diese Option stellt eine zweite Verteidigungslinie für die Autorisierung von Prozessen im Ordner "Systemstart" bereit. HIPS überwacht den Inhalt des Startordners und wenn es einen neuen Prozess findet, wird die von Ihnen ausgewählte Aktion ausgeführt ("Alarmieren und zur Durchführung einer Aktion auffordern", "Die Ausführung des Programms immer zulassen" oder "Ohne Alarmierung vom Start entfernen").

- **Als Standard festlegen:** Weist diese Einstellung als die Standardeinstellung für Tasks zu, die HIPS-Einstellungen verwenden.
- **Kennung:** Identifiziert diese spezifische Einstellung. Diese Information wird in der Datenbank gespeichert und kann zur Nachverfolgung der Einstellungen verwendet werden.
- **Speichern:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Informationen zum Dialogfeld "HIPS: Moduskonfiguration"

Diese Seite verwenden Sie zur Konfiguration des Betriebsmodus für den HIPS-Schutz.

Diese Seite enthält folgende Optionen:

- **Host Intrusion Prevention-Modus:** Legt das Schutzverhalten bei aktiviertem HIPS-Schutz fest. Wenn der HIPS-Modus aktiviert ist, können Sie eine der folgenden Methoden für den Betrieb wählen.
    - **Blockierung:** Sicherheitsverletzungen werden blockiert und in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
    - **Erfassung:** Alle Sicherheitsverstöße sind zulässig, aber das Anwendungsverhalten wird beobachtet ("erfasst") und diese Informationen werden in Form einer Liste der vertrauenswürdigen Dateien an die Coredatenbank zurückgesendet. Verwenden Sie diesen Modus zum Erkennen des Anwendungsverhaltens auf einem bestimmten Gerät oder Gerätegruppe und nutzen diese Informationen dann zur Erstellung benutzerdefinierter HIPS-Richtlinien, bevor Sie diese bereitstellen und den HIPS-Schutz im Netzwerk durchsetzen.
    - **Nur protokollieren:** Sicherheitsverletzungen sind zulässig und werden in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
    - **Lautlos:** Sicherheitsverletzungen werden blockiert und NICHT in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
- **Positivlisten-Modus:** Legt das Schutzverhalten bei aktiviertem Positivlistenschutz fest. Positivlistenschutz bedeutet, dass nur Anwendungen, die in einer Liste der vertrauenswürdigen Dateien stehen und mit der Positivlistenkennzeichnung versehen sind (d. h. Anwendungen, bei denen in der Dateizertifizierung die Option "Ausführung zulassen" aktiviert ist), ausgeführt werden dürfen und erfasst werden. Wenn der Positivlisten-Modus aktiviert ist, können Sie eine der folgenden Methoden für den Betrieb wählen.
    - **Blockierung:** Sicherheitsverletzungen werden blockiert und in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
    - **Erfassung:** Alle Sicherheitsverstöße sind zulässig, aber das Anwendungsverhalten wird beobachtet ("erfasst") und diese Informationen werden in Form einer Liste der vertrauenswürdigen Dateien an die Coredatenbank zurückgesendet. Verwenden Sie diesen Modus zum Erkennen des Anwendungsverhaltens auf einem bestimmten Gerät oder Gerätegruppe und nutzen diese Informationen dann zur Erstellung benutzerdefinierter HIPS-Richtlinien, bevor Sie diese bereitstellen und den HIPS-Schutz im Netzwerk durchsetzen.
    - **Nur protokollieren:** Sicherheitsverletzungen sind zulässig und werden in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
    - **Lautlos:** Sicherheitsverletzungen werden blockiert und NICHT in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.

Informationen zum Dialogfeld "HIPS: Dateischutzregeln"

Diese Seite verwenden Sie zum Anzeigen, Verwalten und Priorisieren von Dateischutzregeln. Dateischutzregeln sind Beschränkungen, die bestimmte Ausführungsdateien daran hindern, gewisse Aktionen auf angegebenen Dateien durchzuführen. Sie können mit Dateischutzregeln Zugriff, Änderung, Erstellung und Ausführung jedes Programms in jeder Datei zulassen oder verweigern.

Dieses Dialogfeld enthält folgende Optionen:

- **Schutzregeln:** Führt alle von LANDesk vordefinierten (Standard) Dateischutzregeln auf, sowie alle von Ihnen erstellten Dateischutzregeln.
  - **Regelname:** Bezeichnet die Dateischutzregel.
  - **Beschränkungen:** Zeigt die spezifischen Aktionen von Programmen in Dateien an, die durch eine Dateischutzregel geschützt sind.
  - **Programme:** Zeigt die Ausführungsprogramme an, die von der Schutzregel geschützt werden.
- **Nach oben \ unten:** Bestimmt die Priorität der Dateischutzregel. Eine Dateischutzregel, die an höherer Stelle auf der Liste steht, hat Vorrang vor einer Regel, die weiter unten steht. Sie können z. B. eine Regel erstellen, die verhindert, dass ein Programm auf eine bestimmte Datei oder Dateiart zugreifen oder sie ändern kann, dann jedoch noch eine weitere Regel erstellen, die eine Ausnahme zu dieser Beschränkung für ein oder mehrere angegebene Programme bildet. Solange die zweite Regel an höherer Stelle auf der Regelliste steht, ist sie wirksam.
- **Zurücksetzen:** Stellt von LANDesk vordefinierte (Standard) Dateischutzregeln wieder her.
- **Hinzufügen:** Öffnet das Dialogfeld "Dateischutzregel konfigurieren", in dem Sie Programme und Dateien hinzufügen und entfernen sowie Beschränkungen angeben können.
- **Bearbeiten:** Öffnet das Dialogfeld "Dateischutzregel konfigurieren", in dem Sie eine bestehende Dateischutzregel bearbeiten können.
- **Löschen:** Entfernt die Dateischutzregel aus der Datenbank.

HINWEIS: Dateischutzregeln werden in der Datei FILEWALL.XML gespeichert, die Sie hier finden: Programme\Landesk\ManagementSuite\ldlogon\AgentBehaviors\Hips_Behavior.ZIP.

Informationen zum Dialogfeld "HIPS: Dateischutzregel konfigurieren"

Auf dieser Seite konfigurieren Sie Dateischutzregeln.

Dieses Dialogfeld enthält folgende Optionen:

- **Regelname:** Bestimmt die Dateischutzregel durch einen beschreibenden Namen.
- **Überwachte Programme:**
  - **Alle Programme:** Gibt an, dass keines der ausführbaren Programme die nachstehend ausgewählten Aktionen für die nachstehend angegebenen Dateien ausführen darf.
  - **Benannte Programme:** Gibt an, dass die nachfolgend ausgewählten Beschränkungen nur für die ausführbaren Programme in dieser Liste gelten.
  - **Hinzufügen:** Sie können auswählen, welche Programme durch die Dateischutzregel beschränkt werden. Sie können Dateinamen und Platzhalter verwenden.
  - **Bearbeiten:** Gestattet die Bearbeitung des Programmnamens.
  - **Löschen:** Entfernt das Programm aus der Liste.

- **Ausnahmen**
  - **Ausnahmen für zertifizierte Programme zulassen:** Gestattet jedem der ausführbaren Programm auf Ihrer Liste der zertifizierten Dateien, die mit dieser Dateischutzregel verbundene Beschränkung zu umgehen.
- **Dateien schützen**
  - **Jede Datei:** Gibt an, dass alle Dateien vor den o.g. Programmen gemäß ihrer Beschränkungen geschützt sind.
  - **Benannte Dateien:** Gibt an, dass nur die Dateien in der Liste geschützt sind.
  - **Hinzufügen:** Sie können auswählen, welche Dateien durch die Regel geschützt werden. Sie können Dateinamen oder Platzhalter verwenden.
  - **Bearbeiten:** Gestattet die Änderung des Dateinamens.
  - **Löschen:** Entfernt die Datei aus der Liste.
  - **Auch in Unterverzeichnisse übernehmen:** Setzt die Dateischutzregeln in den Unterverzeichnissen eines genannten Verzeichnisses durch.
- **Eingeschränkte Aktionen für geschützte Dateien**
  - **Schreibgeschützter Zugriff:** Verhindert, dass die o. g. Programme auf die geschützten Dateien zugreifen.
  - **Änderung:** Verhindert, dass die o. g. Programme die geschützte Dateien ändern.
  - **Erstellung:** Verhindert, dass die o. g. Programme Dateien erstellen.
  - **Ausführung:** Verhindert, dass die o. g. Programme geschützte Dateien ausführen.

Konfigurieren der LANDesk Firewalleinstellungen

Das neue Extra "LANDesk Firewall" ist eine wichtige Komponente der Endpunktsicherheit, mit der Sie verwaltete Geräte vor nicht autorisierten Anwendungsvorgängen und -verbindungen schützen können.

Mit LANDesk Firewalleinstellungen können Sie vertrauenswürdige Programme (Anwendungen), vertrauenswürdige Netzwerkbereiche und Verbindungsregeln erstellen und konfigurieren, um verwaltete Geräte vor nicht autorisierten Eindringversuchen zu schützen.

WICHTIG: Kompatibilität von LANDesk Firewall und Windows-Firewall
Die LANDesk Firewall ergänzt die Windows-Firewall. Beide Firewalls können gleichzeitig auf verwalteten Geräten aktiviert und ausgeführt werden.

Eine Komponente der Endpunktsicherheit

Die LANDesk Firewall ist eine Komponente der umfassenden Lösung "Endpunktsicherheit", zu der auch die beiden Extras "Host Intrusion Prevention (HIPS)" und "Gerätesteuerung" gehören.

Dieses Kapitel befasst sich mit folgenden Themen:

- "Verwendung der LANDesk Firewalleinstellungen" auf Seite 735
- "Hilfe zu LANDesk Firewalleinstellungen" auf Seite 736

Verwendung der LANDesk Firewalleinstellungen

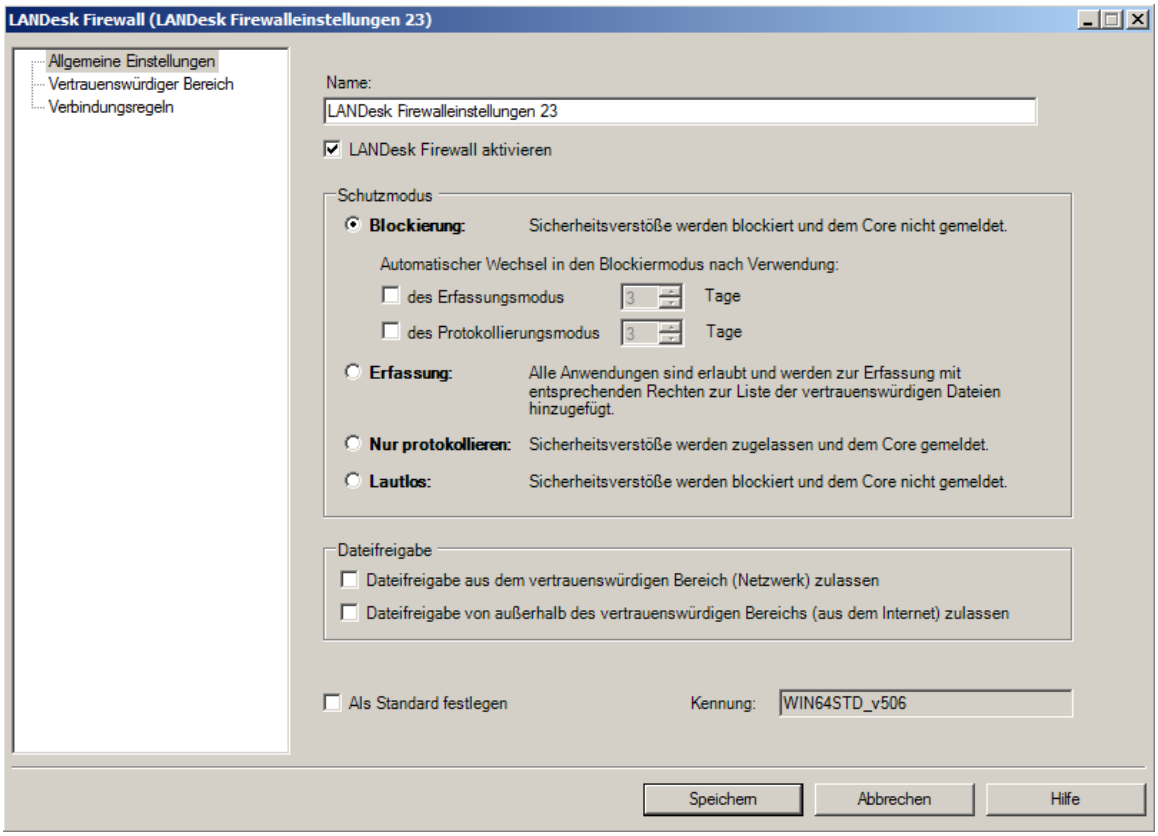
Firewalleinstellungen geben Ihnen vollständige Kontrolle darüber, wie LANDesk Firewall auf Zielgeräten arbeitet.

Dieser Abschnitt beschreibt, wie Firewalleinstellungen erstellt und verwaltet werden.

Erstellen von LANDesk Firewalleinstellungen

So erstellen Sie LANDesk Firewalleinstellungen

1. Klicken Sie im Fenster des Extras **Agenteneinstellungen** mit der rechten Maustaste auf **LANDesk Firewall** und klicken Sie dann auf **Neu**.



2. Geben Sie auf der Seite **Allgemeine Einstellungen** einen Namen für die Einstellungen ein, aktivieren Sie den LANDesk Firewalldienst und geben Sie dann den Schutzmodus an. Wenn Sie Informationen zu einer Option benötigen, klicken Sie auf **Hilfe**.
3. Auf der Seite **Listen der vertrauenswürdigen Dateien** können Sie die ausführbaren Dateien von Anwendungen hinzufügen und bearbeiten, zu denen Sie eine Verbindung vom Netzwerk und vom Internet aus herstellen wollen. Außerdem können Sie den vertrauenswürdigen Bereich definieren.
4. Auf der Seite **Verbindungsregeln** definieren Sie die Verbindungsregeln (Eingehend oder Ausgehend und Aktion) entweder über den Port, das Protokoll oder den IP-Bereich.
5. Klicken Sie auf **Speichern**.

Nachdem Sie die Einstellungen konfiguriert haben, können Sie diese über einen Installations- oder Updatetask oder mithilfe eines Tasks zum Ändern von Einstellungen auf verwaltete Geräte übertragen.

Hilfe zu LANDesk Firewalleinstellungen

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten von LANDesk Firewalleinstellungen. Bei der Erstellung von Firewalleinstellungen definieren Sie zunächst den allgemeinen Schutzmodus. Anschließend fügen Sie spezifische Listen vertrauenswürdiger Dateien, vertrauenswürdige Bereiche und Verbindungsregeln hinzu und konfigurieren diese. Sie können beliebig viele Einstellungen erstellen und jederzeit bearbeiten.

Wenn Sie die Standardeinstellungen des Geräts ändern möchten, ohne den Agenten für Endpunktsicherheit erneut zu installieren oder erneut eine vollständige Agentenkonfiguration bereitzustellen, sollten Sie die gewünschte Änderung an einer der Optionen im Dialogfeld "Einstellungen" vornehmen, die neuen Einstellungen einem Einstellungsänderungs-Task zuordnen und diesen Einstellungsänderungs-Task dann auf Zielgeräten bereitstellen.

Dieses Dialogfeld umfasst die folgende Seiten:

Informationen zur Seite "Allgemeine Einstellungen"

Diese Seite verwenden Sie, um die LANDesk Firewall zu aktivieren und den Schutzmodus zu konfigurieren.

Diese Seite enthält folgende Optionen:

- **Name:** Kennzeichnet die Firewalleinstellungen mit einem eindeutigen Namen.
- **LANDesk Firewall aktivieren:** Alle Programme dürfen ausgeführt werden, es sei denn, der Einsatz eines Programms gefährdet laut vordefinierter Schutzregeln die Systemsicherheit.
- **Schutzmodus:** Gibt das Schutzverhalten an, wenn Sicherheitsverletzungen auf verwalteten Geräten auftreten.
    - **Automatikmodus:** Alle Sicherheitsverletzungen werden automatisch blockiert. Dies bedeutet, dass alle vertrauenswürdigen Programme, der vertrauenswürdige Bereich und die Verbindungsregeln (d. h. die Berechtigungen), die Sie erstellt haben, durchgesetzt werden.
        - **Erfassungsmodus für:** Damit kann der Administrator eine bestimmte Zeitspanne angeben, in der der Endbenutzer jede Anwendung auf seinem Gerät ausführen kann. In dieser Zeitspanne beobachtet das System, welche Anwendungen ausgeführt werden.

          HINWEIS: Diese beiden Optionen für die Dauer werden nacheinander ausgeführt. Dies bedeutet Folgendes: Wenn beide Optionen gewählt werden, verstreicht zunächst die für den Erfassungsmodus definierte Zeit und wenn diese vorüber ist, beginnt der für den Überwachungsmodus definierte Zeitraum.

        - **Überwachungsmodus für:** Definiert einen Zeitraum, innerhalb dessen die Anwendungen, die ausgeführt werden, in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet werden.
    - **Erfassungsmodus:** Alle Anwendungen dürfen ausgeführt werden. Darüber hinaus werden alle Anwendungen, die auf dem Gerät ausgeführt werden, beobachtet und zur Liste der vertrauenswürdigen Dateien hinzugefügt.
    - **Überwachungsmodus:** Sicherheitsverletzungen sind zulässig, werden aber in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.

    - **Blockmodus:** Sicherheitsverletzungen werden blockiert und nicht in einer Aktionsverlaufsdatei auf dem Coreserver aufgezeichnet.
- **Dateifreigabe:** Gibt die Dateifreigabe-Berechtigungen an, die von den LANDesk Firewalleinstellungen zugelassen werden.
    - **Dateifreigabe aus dem vertrauenswürdigen Bereich (Netzwerk) zulassen:** Gestattet die Freigabe von Dateien innerhalb des von Ihnen definierten vertrauenswürdigen Bereichs.
    - **Dateifreigabe von außerhalb des vertrauenswürdigen Bereichs (aus dem Internet) zulassen:** Gestattet die Freigabe von Dateien außerhalb des von Ihnen definierten vertrauenswürdigen Bereichs.

Informationen zur Seite "Listen der vertrauenswürdigen Dateien"

Diese Seite verwenden Sie für die Erstellung und Verwaltung von Listen vertrauenswürdiger Dateien und vertrauenswürdiger Bereiche.

Diese Seite enthält folgende Optionen:

- **Listen der vertrauenswürdigen Dateien:** Zeigt die Dateilisten, die Dateien mit für HIPS konfigurierte Rechte aufweisen.
    - **Hinzufügen:** Öffnet das Dialogfeld **Listen der vertrauenswürdigen Dateien konfigurieren**, in dem Sie Ihre Listen der vertrauenswürdigen Dateien verwalten können.
    - **Bearbeiten:** Hiermit können Sie die Liste der vertrauenswürdigen Dateien bearbeiten.
    - **Entfernen:** Hiermit können Sie die Liste der vertrauenswürdigen Dateien entfernen.
- **Optionen für Erfassungsaktivität:** Gibt an, wie Dateiaktivität behandelt wird, wenn der Schutzmodus auf Erfassung eingestellt ist.
    - **Erfassungsliste:** Zeigt die Liste der vertrauenswürdigen Dateien an, auf die die erfasste Dateiaktivität angewendet wird.
    - **Erfassungsaktivität nur zur Erfassungsliste hinzufügen:** Beschränkt die erfasste Dateiaktivität auf die angegebene Dateiliste.
    - **Erfassungsaktivität zu jeder Liste hinzufügen, in der dieselbe Datei bereits enthalten ist:** Die erfasste Dateiaktivität kann auf jede Dateiliste angewendet werden, die diese Datei enthält.
- **Vertrauenswürdiger Bereich:** Listet die Netzwerkbereiche, deren Verbindungsregeln für Firewallschutz konfiguriert sind.

Informationen zum Dialogfeld "Vertrauenswürdige Anwendung konfigurieren"

Diese Seite verwenden Sie zum Konfigurieren von Verbindungsregeln für eine bestimmte Anwendung.

Diese Seite enthält folgende Optionen:

- **Anwendungsdetails:** Kennzeichnet die Anwendungsdatei, der Verbindungsregeln (d. h. Berechtigungen) zugewiesen werden. Sie können eine Beschreibung für die Registrierungsdatei eingeben.

- **Ausgehende Verbindung**
  - **Anwendungen dürfen Verbindungen zum vertrauenswürdigen Bereich (Netzwerk) herstellen:** Gestattet es Anwendungen, Verbindungen zu Speicherorten herzustellen, die innerhalb des von Ihnen definierten vertrauenswürdigen Bereichs liegen.
  - **Anwendungen dürfen Verbindungen außerhalb des vertrauenswürdigen Bereichs (zum Internet) herstellen:** Gestattet es Anwendungen, Verbindungen zu Speicherorten herzustellen, die außerhalb des von Ihnen definierten vertrauenswürdigen Bereichs liegen.
- **Eingehende Verbindung**
  - **Aus dem vertrauenswürdigen Bereich (Netzwerk) dürfen Verbindungen zu Anwendungen hergestellt werden:** Gestattet es Anwendungen, Verbindungen von Speicherorten entgegenzunehmen, die innerhalb des von Ihnen definierten vertrauenswürdigen Bereichs liegen.
  - **Von außerhalb des vertrauenswürdigen Bereichs (aus dem Internet) dürfen Verbindungen zu Anwendungen hergestellt werden:** Gestattet es Anwendungen, Verbindungen von Speicherorten entgegenzunehmen, die außerhalb des von Ihnen definierten vertrauenswürdigen Bereichs liegen.
- **Vertrauenswürdige Anwendungen sperren:** Stellt sicher, dass die Anwendung die von Ihnen an dieser Stelle zugewiesenen Verbindungsregeln beibehält, selbst wenn die Anwendung während eines Lernvorgangs im Erfassungsmodus andere Operationen ausführen darf.
- **OK:** Speichert die Verbindungsregeln und fügt die Anwendung zur Liste der vertrauenswürdigen Programme hinzu.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Informationen zum Dialogfeld "Vertrauenswürdiger Bereich"

Diese Seite verwenden Sie zur Konfiguration und Verwaltung von vertrauenswürdigen Bereichen. Ein vertrauenswürdiger Bereich besteht aus einer Sammlung von Netzwerkadressen nach IP-Adresse, IP-Bereich oder Subnetz.

Diese Seite enthält folgende Optionen:

- **Dem Subnetz des Clients vertrauen:** Fügt den Subnetzbereich des Zielgeräts zur Liste "Vertrauenswürdiger Bereich" hinzu. Die Kommunikation über diesen Subnetzbereich hinweg ist zulässig.
- **Vertrauenswürdige Bereiche:** Listet alle vertrauenswürdigen Bereiche auf.
- **Importieren:** Gibt Ihnen die Möglichkeit, Subnetzbereiche von verwalteten Geräten zu importieren, die im Inventar der Coredatenbank enthalten sind.
- **Hinzufügen:** Gibt Ihnen die Möglichkeit, einen vertrauenswürdigen Speicherort zur Liste hinzuzufügen. Fügen Sie einen vertrauenswürdigen Speicherort nach IP-Adresse, IP-Bereich oder Subnetz hinzu.
- **Bearbeiten:** Gibt Ihnen die Möglichkeit, den ausgewählten vorhandenen vertrauenswürdigen Speicherort zu ändern.
- **Löschen:** Entfernt den ausgewählten vertrauenswürdigen Speicherort.

Informationen zum Dialogfeld "Verbindungsregeln"

Diese Seite verwenden Sie zum Anzeigen, Verwalten und Priorisieren von Verbindungsregeln. Verbindungsregeln gestatten oder unterbinden Verbindungen auf der Basis von Port- oder IP-Bereichen oder je nachdem, ob das Programm vertrauenswürdig ist und ob die Kommunikation innerhalb des vertrauenswürdigen Netzwerkbereichs erfolgt.

Diese Seite enthält folgende Optionen:

- **Verbindungsregeln:** Listet alle Verbindungsregeln auf.
- **Nach oben:** Bestimmt die Priorität der Verbindungsregel. Eine Verbindungsregel, die an höherer Stelle auf der Liste steht, hat Vorrang vor einer Regel, die weiter unten steht.
- **Nach unten:** Bestimmt die Priorität der Verbindungsregel.
- **Zurücksetzen:** Stellt die Regelreihenfolge wieder her.
- **Hinzufügen:** Öffnet ein Dialogfeld, in dem Sie eine neue Verbindungsregel konfigurieren können.
- **Bearbeiten:** Gestattet die Änderung der ausgewählten Verbindungsregel.
- **Löschen:** Entfernt die ausgewählte Verbindungsregel aus der Datenbank.

Informationen zum Dialogfeld "Verbindungsregel konfigurieren"

Diese Seite verwenden Sie zum Konfigurieren von Verbindungsregeln.

Diese Seite enthält folgende Optionen:

- **Name:** Bestimmt die Verbindungsregel durch einen beschreibenden Namen.
- **Ports:** Dient der Definition von Portbeschränkungen für die Verbindungsregel.
    - **Auf diese lokalen Ports anwenden:** Gibt die lokalen Ports an, auf die die (nachstehend ausgewählte) Richtung und Aktion angewendet werden. Werden zum Beispiel "Eingehend" und "Akzeptieren" ausgewählt, dann sind Verbindungen zu den hier angegebenen lokalen Ports zulässig.
    - **Auf diese Remoteports anwenden:** Gibt die Remoteports an, auf die die (nachstehend ausgewählte) Richtung und Aktion angewendet werden.
- **Protokoll:** Gibt das Kommunikationsprotokoll für die ausgewählten Ports an.
- **IP-Bereich:** Dient zur Definition von IP-Bereichsbeschränkungen für die Verbindungsregel.
    - **Auf diese Remoteadressen anwenden:** Gibt die Remote-IP-Adressbereiche an, auf die die (nachstehend ausgewählte) Richtung und Aktion angewendet werden.
- **Richtung:** Gibt an, ob die Verbindungsregel eingehende oder ausgehende Verbindungen beschränkt.
- **Aktion:** Gibt an, ob die Verbindungsregel Verbindungen zulässt (annimmt) oder verhindert (trennt).
- **Vertrauenswürdigen Programmen Umgehung gewähren:** Hiermit können Sie vertrauenswürdigen Programmen die Möglichkeit einräumen, diese Verbindungsregel zu ignorieren oder zu umgehen.
    - **Nur für vertrauenswürdigen Bereich:** Vertrauenswürdige Programme können die Verbindungsregel nur dann umgehen, wenn die Kommunikation innerhalb des vertrauenswürdigen Netzwerkbereichs erfolgt.
- **OK:** Speichert die Optionen und fügt die Regel zur Liste der Verbindungsregeln hinzu.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Gerätesteuerung – Übersicht

Das neue Extra "Gerätesteuerung" ist eine wichtige Komponente der Endpunktsicherheit, mit der Sie den Zugriff für E/A-Geräte überwachen und beschränken können. Mit der Gerätesteuerung können Sie die Nutzung von Geräten beschränken, die einen Datenzugriff auf das Gerät gestatten, wie z. B. Ports, Modems, Laufwerke und Wireless-Verbindungen.

Zur Implementierung der Gerätesteuerung auf Clients in Ihrem Netzwerk erstellen Sie Gerätesteuerungseinstellungen zur Verwaltung von USB- und Modem-Verbindungen, E/A-Ports, CD/DVD-Laufwerken, PCMCIA- und anderen Verbindungen und stellen diese bereit.

Sie können USB-Beschränkungen konfigurieren, indem Sie entweder eine ganze USB-Geräteklasse (z. B. Speichergeräte) oder nur bestimmte USB-Geräte blockieren, indem Sie Ausnahmen auf der Basis von Parametern und Werten, die Sie angeben, definieren.

Eine Komponente der Endpunktsicherheit

Die Gerätesteuerung ist eine Komponente der umfassenden Lösung "Endpunktsicherheit", zu der auch die beiden Extras "Host Intrusion Prevention (HIPS)" und "LANDesk Firewall" gehören.

Unterstützte Plattformen

Die Gerätesteuerung unterstützt verwaltete Geräte mit folgenden Betriebssystemen:

- Windows 2000
- Windows Server 2003
- Windows XP
- Windows Vista (32-Bit und 64-Bit)
- Windows 7

Beschränken des Gerätezugriffs mit Gerätesteuerungseinstellungen

Damit die Gerätesteuerung auf einem Gerät ausgeführt werden kann, müssen auf dem betreffenden Gerät der Local Scheduler Agent und der Standardagent bereitgestellt werden. Immer, wenn das Gerät eine Geräteverbindung aufbaut oder Änderungen an einer Geräteverbindung vornimmt, wendet der Agent Einstellungsregeln an. Zu diesen Regeln gehört das Trennen unzulässiger Verbindungen und Alarmieren des Coreservers.

Standardmäßig können die Einstellungen für die Gerätesteuerung den Zugriff auf die unterschiedlichsten Gerätetypen beschränken. Sie können mithilfe der erweiterten USB-Einstellungen für jedes USB-Gerät oder für jede Geräteklasse, die Sie angeben, Zugriffsbeschränkungen definieren. Zu den Gerätetypen, für die Zugriffsbeschränkungen festgelegt werden können, gehören:

- USB-Geräte wie Laufwerke, Tastaturen, Mäuse, Drucker und Scanner
- RIM Blackberry, Pocket PC und Palm-Handheldgeräte
- Netzwerkvolumes
- Personal Area Networks mit Bluetooth
- Wireless 802.11x-Netzwerke
- Modems
- PCMCIA-Geräte

- Serielle Anschlüsse sowie Parallel-, Infrarot- und FireWire 1394-Anschlüsse
- Diskettenlaufwerke und CD/DVD-Laufwerke

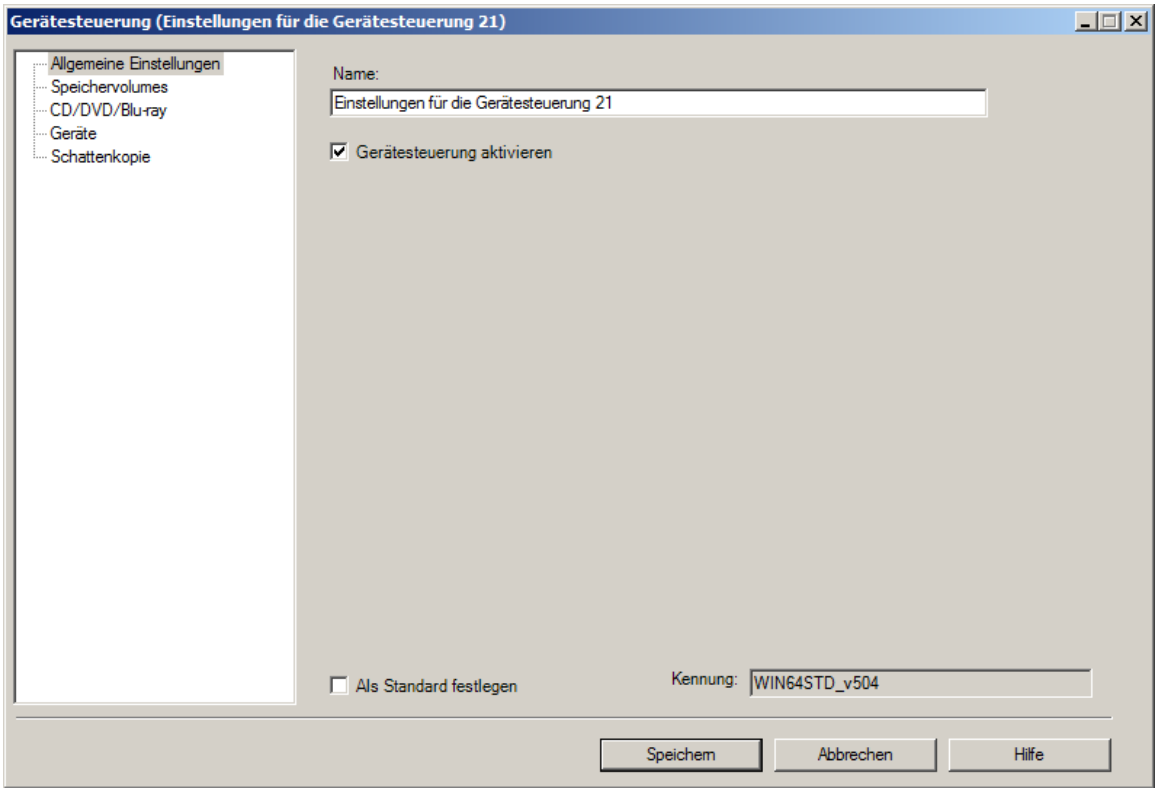
Die Konfiguration für die USB-Gerätekontrolle verwendet den Dienst "LANDesk Endpunktsicherheit", der Folgendes ermöglicht:

- Die Verwendung nicht autorisierter USB- und PCMCIA-Geräte verhindern.
- Die Verwendung nicht autorisierter Wechselspeichermedien verhindern.
- Beim Erkennen eines nicht autorisierten Gerätes ein externes Programm oder Skript starten.

Erstellen von Einstellungen für die Gerätesteuerung

So erstellen Sie Einstellungen für die Gerätesteuerung

1. Klicken Sie auf **Extras > Sicherheit > Sicherheitskonfigurationen**.
2. Öffnen Sie die Endpunktsicherheit, klicken Sie mit der rechten Maustaste auf **Gerätesteuerung** und klicken Sie dann auf **Neu**.



3. Geben Sie auf der Seite "Allgemeine Einstellungen" einen **Namen** ein.
4. Aktivieren Sie das Kontrollkästchen **Gerätesteuerung aktivieren**.
5. Passen Sie die Optionen auf den anderen Seiten Ihren Vorstellungen entsprechend an. Nähere Informationen zu den Optionen in diesem Dialogfeld finden Sie unter "Hilfe zu den Einstellungen für die Gerätesteuerung" auf Seite 748.
6. Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

Bereitstellen von Einstellungen für die Gerätesteuerung

Nachdem Sie eine Einstellung für die Gerätesteuerung erstellt haben, müssen Sie diese auf verwalteten Geräten bereitstellen, damit sie aktiviert wird.

Die Gerätesteuerung wird über die Einstellungen für die Endpunktsicherheit bereitgestellt.

So stellen Sie Einstellungen für die Gerätesteuerung bereit

1. Klicken Sie mit der rechten Maustaste auf die Einstellung und klicken Sie dann auf **Planen**.
2. Die Einstellung wird zum Fenster **Geplante Tasks** hinzugefügt. Ziehen Sie in diesem Fenster angezeigte Geräte auf das Einstellungssymbol.
3. Klicken Sie vom Kontextmenü des Tasks auf **Eigenschaften**, nachdem Sie alle Geräte hinzugefügt haben. Klicken Sie in der Strukturansicht auf **Geplanten Task** und konfigurieren Sie die Zeitplanoptionen.

Weitere Informationen über die Taskplanung finden Sie unter "Planen von Tasks" auf Seite 242.

Wenn Sie die Bereitstellung von Einstellungen für die Gerätesteuerung planen, führt die Gerätesteuerung die folgenden Schritte aus:

- Sie erstellt ein ausführbares Verteilungspaket, das nach den Einstellungen für die Gerätesteuerung benannt wird. Die primäre Datei des Pakets ist ldsecsvc.exe. Zu den zusätzlichen Dateien gehören ldsecsvc.reg, devactalert.exe, netres.mrl und <*Name der Einstellungen für die Gerätesteuerung*>.ini.
- Wenn Sie Benutzer als Ziel für den Task "Einstellungen für die Gerätesteuerung" auswählen, verwendet die Gerätesteuerung eine öffentliche richtlinienbasierte Verteilungsmethode mit dem Namen "LANDesk Endpunktsicherheit – Pullverteilung". Wenn die Verteilungsmethode nicht existiert, wird sie von der Gerätesteuerung erstellt. Wenn es sich bei den Taskzielen um Benutzer handelt, muss die Gerätesteuerung eine richtlinienbasierte Methode verwenden, um sicherzustellen, dass der vorgesehene Benutzer die Einstellungen erhält. Wenn als Ziel angesprochene Benutzer sich anmelden, aktiviert und installiert die richtlinienbasierte Verteilungsmethode die Einstellungen.
- Wenn Sie Computer als Ziel für den Einstellungstask für die Gerätesteuerung auswählen, verwendet die Gerätesteuerung eine öffentliche richtlinienunterstützte Pushverteilungsmethode mit dem Namen "LANDesk Endpunktsicherheit – Pushverteilung". Wenn die Verteilungsmethode nicht existiert, wird sie von der Gerätesteuerung erstellt. Da die Einstellungen als Ziel ein Gerät ansprechen, erhält jeder Benutzer, der sich bei dem betreffenden Gerät anmeldet, diese Einstellungen für die Gerätesteuerung; es spielt keine Rolle, wer beim Installieren der Einstellungen angemeldet ist. Sie können pushbasierte oder richtlinienbasierte Liefermethoden für Computer verwenden.

Nachdem die Gerätesteuerung die richtlinienbasierte Pullverteilungsmethode bzw. richtlinienunterstützte Pushverteilungsmethode erstellt hat, können Sie diese anpassen. Solange der Name der Methode sich nicht ändert, verwendet die Gerätesteuerung die geänderte Verteilungsmethode.

Erstellen von benutzerdefinierten Meldungen zur Benachrichtigung beim Erkennen nicht autorisierter Geräte oder Volumes

Sie können im Dialogfeld **Einstellungen für die Gerätesteuerung** einen Meldungstext entwerfen, der auf dem Bildschirm des Benutzers beim Erkennen nicht autorisierter Geräte oder Volumes angezeigt wird. In diesen Meldungstext können Sie mithilfe der folgenden Platzhalter das nicht autorisierte Volume bzw. das nicht autorisierte Gerät betreffende Informationen anzeigen:

- %vol%: Seriennummer des Volumes
- %desc%: Beschreibung
- %service%: Dienst
- %hwid%: Hardwarekennung
- %mfg%: Hersteller
- %loc%: Speicherort
- %class%: Klasse

Andere Verwaltungstasks zur Gerätesteuerung

Die nachstehenden Themen bieten Informationen zu den folgenden Funktionen und Tasks der Gerätesteuerung:

- Handhabung nicht autorisierter Geräte
- Handhabung von Wechselspeichermedien
- Konfigurieren erweiterter USB-Einstellungen
- Konfigurieren von Befehlen, die beim Erkennen nicht autorisierter Geräte ausgeführt werden
- Konfigurieren von Gerätesteuerungsalarmen
- Anzeigen der Liste mit den nicht autorisierten Geräten

Handhabung nicht autorisierter Geräte

Die Einstellungen für die Gerätesteuerung verwenden auf verwalteten Geräten den Dienst "LANDesk Endpunktsicherheit". Wenn der Dienst vom Betriebssystem die Nachricht erhält, dass ein neues USB- oder PCMCIA-Gerät hinzugefügt wurde, entscheidet der Dienst anhand von mehreren benutzerdefinierten Regeln, ob es sich um ein zulässiges Gerät handelt oder nicht. Mithilfe einfacher Regeln, die Sie selbst erstellen können, kann der Zugriff auf Geräte wie Tastatur und Maus, Drucker und Scanner beschränkt werden. Komplexere Regeln bieten die Möglichkeit, den Zugriff gezielter zu steuern, indem Sie beispielsweise nur die sicheren Speichergeräte eines bestimmten Herstellers zulassen oder die Geräte eines bestimmten Herstellers ausschließen.

Wenn ein nicht autorisiertes Gerät erkannt wird, veranlasst der Dienst "LANDesk Endpunktsicherheit" Folgendes:

- Das Gerät wird aus dem Windows-Gerätemanager entfernt, damit es von Windows nicht mehr erkannt wird. Alle etwaigen Treiber für das Gerät bleiben installiert.
- Bei einem nicht autorisierten USB-Gerät oder -Volume wird auf dem Bildschirm des Benutzers optional eine konfigurierbare Meldung angezeigt. Weitere Informationen finden Sie unter "Erstellen von benutzerdefinierten Meldungen zur Benachrichtigung beim Erkennen nicht autorisierter Geräte/Volumes".
- Optional wird ein externes Programm geladen (weitere Informationen finden Sie unter Konfigurieren von Befehlen, die beim Erkennen nicht autorisierter Geräte ausgeführt werden). Das externe Programm kann beispielsweise ein Skript sein, das einen Alarm an eine zentrale Konsole sendet.
- Senden Sie einen "Deaktiviertes Gerät aktiviert" AMS-Alarm an den Coreserver. Die Alarmnachricht schließt den Gerätenamen ein.

Handhabung von Wechselspeichermedien

USB-Verbindungen auf verwalteten Geräten werden durch einen Dienst namens "LANDesk Endpunktsicherheit" beschränkt. Beim Aktivieren eines neuen Volumes benachrichtigt das Betriebssystem den Dienst. Der Dienst verwendet dann den GetDriveType() API-Aufruf, um den Typ des Laufwerks zu überprüfen, das aktiviert wurde. Wenn das Betriebssystem das Laufwerk als "austauschbar" oder als "fest installiertes Laufwerk" beschreibt, führt der Dienst Aktionen aus. Außerdem überprüft der Dienst das System beim Starten auf das Vorhandensein von Wechselmedien. Wird beim Starten ein nicht autorisiertes Volume gefunden, so werden dieselben Aktionen wie beim späteren Aktivieren des Volumes ausgeführt.

Zu den Laufwerken, die als austauschbar eingestuft werden, gehören u.a. auch USB-Speichergeräte. CD-Laufwerke (schreibgeschützt oder mit Lese-/Schreibzugriff) zählen nicht zu den austauschbaren Speichergeräten.

Das Betriebssystem zählt Festplattenlaufwerke nicht zu den austauschbaren Speichergeräten. Diese werden vom Aufruf "GetDriveType()" als "fest installiert" beschrieben, selbst wenn sie über einen USB-Port oder einen anderen externen Port mit dem System verbunden sind. Um zu veranlassen, dass austauschbare Festplattenlaufwerke genauso gehandhabt werden wie andere austauschbare Speichergeräte, zeichnet der Dienst die Liste mit den Festplattenlaufwerken beim Installieren des Dienstes auf. Wenn ein Gerät zum Zeitpunkt der Installation des Dienstes z. B. zwei Festplatten enthält (C: und D:), sieht der Dienst diese Laufwerke als fest installierte Laufwerke an und schließt sie von der Überprüfung aus. Wenn aber zu einem späteren Zeitpunkt ein Festplattenlaufwerk mit dem Laufwerksbuchstaben E: gefunden wird, stuft der Dienst dieses Laufwerk als austauschbares Speichergerät ein.

Der Dienst "LANDesk Endpunktsicherheit" speichert die Liste mit den fest installierten Laufwerken in der Registrierung unter HKLM\Software\LANDesk\usbmon\FixedDrives. Diese Liste wird beim Installieren des Dienstes erstellt. Die Option **Kein Zugriff** blockiert den Zugriff auf alle Volumes, die nicht vorhanden waren, als die Einstellungen für die Gerätesteuerung installiert wurden. Hinweis: Wenn ein Gerät, das ein Volume enthält, beim Installieren der Einstellungen angeschlossen war, lässt der Dienst das Gerät künftig zu, obwohl es sich möglicherweise um ein Wechselmedium handelt.

Wenn ein austauschbares Speichergerät erkannt wird, veranlasst der Dienst "LANDesk Endpunktsicherheit" Folgendes:

- Sperrung des Volumes. Benutzer, die versuchen, auf das Volume zuzugreifen, erhalten die Fehlermeldung "Zugriff verweigert".
- Optional wird auf dem Bildschirm des Benutzers eine konfigurierbare Meldung eingeblendet.
- Optional wird ein externes Programm geladen. Das externe Programm kann beispielsweise ein Skript sein, das einen Alarm an eine zentrale Konsole sendet.
- Senden Sie einen "Deaktiviertes Gerät aktiviert" AMS-Alarm an den Coreserver. Der Alarm meldet, dass ein Volume aktiviert wurde, jedoch keine zusätzlichen Informationen zu diesem Volume verfügbar sind.

WICHTIG: Die Blockierung von sämtlichen unbekannten Volumes wird nur unter Windows XP oder Windows 2003 unterstützt
Unter Windows 2000 meldet das Betriebssystem, dass das Volume blockiert ist, obwohl dies nicht der Fall ist. Wir empfehlen Ihnen, für Windows 2000 spezifische Geräte zu blockieren, um das Hinzufügen neuer Volumes zu verhindern.

Was tun, wenn ein Supportmitarbeiter einen USB Memory Stick verwenden muss?

Wenn Sie als Mitarbeiter eines IT-Supportteams ein USB-Speichergerät auf dem Computer eines Benutzers verwenden möchten, haben Sie mehrere Möglichkeiten:

- Die praktischste Methode, temporären Zugriff auf ein USB-Gerät zu ermöglichen, besteht darin, beim Definieren und Bereitstellen von Einstellungen für die Gerätesteuerung auf Ihren verwalteten Geräten die Option zur Außerkraftsetzung des Kennwortes zu aktivieren.

Sie können folgende Methoden ausprobieren, wenn die Gerätesteuerung nicht mit der Funktion zum Außerkraftsetzen des Kennwortes konfiguriert wurde:

- Melden Sie sich mit Admin-Rechten an und deaktivieren Sie den Dienst "LANDesk Endpunktsicherheit" vorübergehend.
- Melden Sie sich mit Admin-Rechten an, führen Sie die Dienst-GUI von LANDesk Endpunktsicherheit aus und fügen Sie das Gerät in die Liste der autorisierten Volumes ein.

Konfigurieren erweiterter USB-Einstellungen

Sobald die Gerätesteuerung auf einem Gerät installiert ist, speichert der Agent Informationen zu den letzten zehn USB-Geräten, für die er den Zugriff gesperrt hat. Der Inventarscanner sendet diese Informationen an die Coredatenbank. Informationen zu diesen blockierten Geräten werden dann im Dialogfeld **Erweiterte USB-Einstellungen** angezeigt. Sie können diese Informationen verwenden, um erweiterte Regeln zu erstellen, die bestimmte USB-Geräte entweder zulassen oder blockieren. Mithilfe von diesen erweiterten Regeln können Sie mehr steuern als nur die einfachen Gerätekategorien, die im Dialogfeld **Einstellungen für die Gerätesteuerung** zu sehen sind.

Im Dialogfeld **Erweiterte USB-Einstellungen** können Sie jede der sechs Spalten als Basis für eine Regel verwenden. Klicken Sie mit der rechten Maustaste auf einen Wert in der Spalte und klicken Sie dann auf **Zulassen**, um eine Regel zu erstellen, die Geräte auf der Basis dieses Attributs zulässt. Die Schlüsselwörter für die einzelnen Spalten lauten wie folgt:

```
DeviceDesc
HardwareID
Dienst
Mfg
LocationInformation
Class
```

Dies sind dieselben Namen, die in der Registrierung unter dem Schlüssel "HKLM\System\CurrentControlSet\Enum\USB" verwendet werden.

Von allen Feldern eignet sich normalerweise das Feld **Dienst** am besten als Ausgangsbasis für Regeln. Dieses Feld entspricht einem Windows-Treiber. Der Name des Treibers für USB ActiveSync-Verbindungen mit Windows CE PDAs lautet beispielsweise wceusbsh (siehe HKLM\CurrentControlSet\Services\wceusbsh). Jede der sechs Spalten kann als Basis für eine Regel verwendet werden; Sie müssen jedoch abhängig von Ihrer Situation selbst entscheiden, welche Regeln in Ihrem Fall sinnvoll sind.

Platzhalter

Sie können Platzhalter in Regeln verwenden. Beispielsweise würde folgende Anweisung alle Geräte zulassen, deren Gerätebeschreibung die Zeichenfolge "floppy" enthält:

```
DeviceDesc=*floppy*
```

Positivlisten-Regeln im Vergleich zu Negativlisten-Regeln

Alle bisher veranschaulichten Regeln waren Positivlisten-Regeln; d. h., die Geräte werden nicht zugelassen, es sei denn, sie erfüllen mindestens eine der Regeln. Der Dienst "LANDesk Endpunktsicherheit" unterstützt jedoch auch Negativlisten-Regeln. Regeln, denen ein Minuszeichen vorangeht, sind Negativlisten-Regeln. Zum Beispiel:

```
Service=usbstor
-DeviceDesc=*floppy*
```

Die erste Regel lässt USB-Speichergeräte zu. Die zweite Regel setzt Geräte, deren Beschreibung die Zeichenfolge "floppy" enthält, auf die Negativliste.

Wenn sowohl Positivlisten- als auch Negativlisten-Regeln definiert werden, gleicht der Dienst Geräte zuerst mit den Positivlisten-Regeln ab. Wenn es keine Positivlisten-Regeln gibt, die das Gerät zulassen, ist das Gerät verboten. Wenn es mindestens eine Positivlisten-Regel gibt, die das Gerät zulässt, gleicht der Dienst das Gerät mit den Negativlisten-Regeln ab. Wenn keine der Negativlisten-Regeln auf das Gerät zutrifft, wird es zugelassen. Andernfalls gilt es als verboten.

Wenn nur Positivlisten-Regeln existieren, gilt das betreffende Gerät als unzulässig, es sei denn, es erfüllt eine der Positivlisten-Regeln. Wenn nur Negativlisten-Regeln existieren, gilt das betreffende Gerät als zulässig, es sei denn, es erfüllt eine der Negativlisten-Regeln.

Zusammengesetzte Regeln

Alle bisher veranschaulichten Regeln waren einfache Regeln, in denen nur ein einzelnes Feld geprüft wird. Dienst "LANDesk Endpunktsicherheit" unterstützt jedoch auch zusammengesetzte Regeln wie die folgende:

```
Service=wceusbsh,DeviceDesc=*iPAQ*
```

Diese Regel lässt nur Windows CE-Geräte zu, in deren Beschreibung die Zeichenfolge IPAQ enthalten ist.

Zusammengesetzte Negativlisten-Regeln werden ebenfalls unterstützt. Beispiel:

```
Service=wceusbsh
-Service=wceusbsh,Mfg=*iPAQ*
```

Die zwei obigen Zeilen lassen alle Windows CE-Geräte zu, mit Ausnahme derjenigen, die die Zeichenfolge IPAQ in ihrem Herstellerfeld aufweisen. Die obigen Zeilen entsprechen der folgenden Einzelzeile:

```
Service=wceusbsh,-Mfg=*iPAQ*
```

Konfigurieren von Befehlen, die beim Erkennen nicht autorisierter Geräte ausgeführt werden

Wenn der Dienst "LANDesk Endpunktsicherheit" nicht autorisierte Datenträger oder Geräte erkennt, kann er externe Programme ausführen. Sie können ein oder zwei Platzhalter in die Befehle einschließen:

- %1: wird entweder durch "volume" oder "device" ersetzt, je nachdem, ob ein nicht autorisiertes Volume oder ein nicht autorisiertes USB-Gerät (device) erkannt wurde.
- %2: wird entweder durch die Seriennummer des nicht autorisierten Volumes oder durch die Kennungszeichenfolge eines nicht autorisierten USB-Geräts ersetzt.

Wenn beispielsweise der folgende Befehl gegeben wird:

```
wscript myscript.vbs %1 %2
```

Dann wird der folgende Befehl gestartet:

```
wscript myscript.vbs volume "1234ABCD"
```

```
wscript myscript.vbs device "Y-E Data USB Floppy: Vid_057b&Pid_0000"
```

Der Dienst gewährleistet, dass immer nur jeweils eine Instanz des Skripts ausgeführt wird.

So konfigurieren Sie Befehle

1. Klicken Sie in der Einstellung für die Gerätesteuerung auf **Befehle**.
2. Geben Sie die gewünschten Befehle ein.
3. Klicken Sie auf **OK**.

Konfigurieren von Gerätesteuerungsalarmen

Die Einstellungen für die Gerätesteuerung verwenden das Alert Management System für die Alarmierung. Die Gerätesteuerung kann für die folgenden Ereignisse Alarme auslösen:

- Konfigurationsfehler
- Deaktiviertes Gerät aktiviert
- Eingeschränkter Netzwerkverbindungsversuch
- Nicht aufgelistete Netzwerkverbindungsversuche
- Nicht in der Liste geführte Netzwerksitzung erkannt

Anzeigen der Liste mit den nicht autorisierten Geräten

Die Gerätesteuerung speichert auf jedem Computer eine Liste mit den letzten zehn nicht autorisierten Geräten, zu denen eine Verbindung hergestellt wurde.

Sie können diese Informationen in der Netzwerkansicht anzeigen, indem Sie im Kontextmenü eines Geräts auf **Inventar** klicken. Klicken Sie dann auf **LANDesk Management >Gerätesteuerung > Alarm**.

Fehlerbehebung für die Gerätesteuerung

In diesem Abschnitt finden Sie Informationen über Probleme, die möglicherweise mit der Gerätesteuerung entstehen können und darüber, wie Sie diese beheben können.

- Jede neue Einstellung für die Gerätesteuerung wird als eine Einstellungsdatei und eine Skriptdatei in folgenden Ordnern gespeichert:
  - ldmain\ccmgr\name.cfg
  - ldmain\scripts\name.ini
- Falls ein Skript oder eine Einstellung existiert, das/die denselben Namen trägt, den Sie für eine Konfiguration vorgesehen haben, werden Sie aufgefordert, das vorhandene Skript bzw. die vorhandene Einstellung zu überschreiben. Bei diesem Vorgang kann ein anderes Verteilungsskript, das denselben Namen trägt, überschrieben werden.
- Schränken Sie beim Eingeben von IP-Bereichen für Netzwerkbeschränkungen nicht den Zugriff für den Netzwerkbereich ein, in dem sich der Coreserver befindet. Wenn Clients auf ein beschränktes Netzwerk zugreifen und die Gerätesteuerung den Netzwerkzugriff deaktiviert, kann der Netzwerkzugriff nur über die Kommunikation mit dem Coreserver wiederhergestellt werden. Wenn Geräte aufgrund einer Beschränkung nicht mit dem Coreserver kommunizieren können, kann der Netzwerkzugriff nicht wiederhergestellt werden.

- Achten Sie beim Beschränken des Zugriffs auf E/A-Geräte darauf, keine E/A-Geräte zu beschränken, die als Host für Netzwerkadapter dienen. Wenn Sie den Zugriff auf E/A-Geräte beschränken, die als Host für einen Netzwerkadapter dienen, kann der betreffende Client nicht mehr auf das Netzwerk zugreifen. Beispiel: Wenn Sie den USB-Zugriff beschränken, funktionieren auch keine USB-Netzwerkadapter mehr. Ohne Netzwerkzugriff können Sie keine Beschränkungseinstellungen für diesen Client aktualisieren.
- Wenn Sie die folgenden Optionen in der Gerätesteuerung wählen und der Coreserver nicht in dem in der Liste geführten Netzwerk verfügbar ist, haben Clients uneingeschränkten E/A-Gerätezugriff, solange sie mit dem betreffenden Netzwerk verbunden sind.
    - Verbindungen auf die in der Liste geführten Netzwerke beschränken
    - Nicht in der Liste geführte Netzwerke zulassen, wenn nicht verbunden
    - Überprüfen, ob Coreserver im Netzwerk existiert
- Wenn die Option "Nicht in der Liste geführte Netzwerke zulassen, wenn nicht verbunden" aktiviert ist und der Agent den Core in einem aufgelisteten Netzwerk nicht findet, wird vom System angenommen, dass es sich um ein nicht aufgelistetes Netzwerk handelt. An diesem Punkt wird u. U. versehentlich Zugriff auf die lokalen E/A-Geräte erteilt. Dies kann ein Sicherheitsrisiko bedeuten. Stellen Sie sicher, dass der Coreserver zur Verfügung steht, um diese Situation zu vermeiden.

Hilfe zu den Einstellungen für die Gerätesteuerung

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten von Einstellungen für die Gerätesteuerung.

Dieses Dialogfeld umfasst die folgende Seiten:

Informationen zur Seite "Allgemeine Einstellungen"

Diese Seite verwenden Sie, um die Einstellungen zu benennen und die Gerätesteuerung auf einem Client zu aktivieren, der mit den Einstellungen konfiguriert ist.

- **Name:** Identifiziert die Einstellungen. Dieser Name wird im Hauptfenster der Gerätesteuerung angezeigt.
- **Gerätesteuerung aktivieren:** Schaltet die Gerätesteuerung auf einem Client ein, der mit den Einstellungen konfiguriert wurde.

Informationen zur Seite "Speichervolumes"

Diese Seite verwenden Sie, um Optionen für Speichervolumes zu definieren, die mit einem Client verbunden werden, der mit dieser Einstellung konfiguriert ist.

- **Speichervolumes:** Gibt die Zugriffsebene für Speichervolumes an, die zum Zeitpunkt der Installation der Einstellung nicht auf dem Client vorhanden waren. (Hinweis: Wenn ein Gerät, das ein Volume enthält, beim Installieren der Einstellungen angeschlossen war, lässt der Dienst "LANDesk Endpunktsicherheit" das Gerät künftig zu, obwohl es sich möglicherweise um ein Wechselmedium handelt.)
    - **Voller Zugriff:** Gewährt einem Speichervolume, zu dem eine Verbindung hergestellt wird, Lese- und Schreibzugriff.
    - **Schreibgeschützter Zugriff:** Gewährt Benutzern schreibgeschützten Zugriff auf ein Speichervolume, zu dem eine Verbindung hergestellt wird.

- **Verschlüsselung verwenden:** Setzt Dateiverschlüsselung auf einem Speichervolume durch, zu dem eine Verbindung hergestellt wird. Es wird ein Verschlüsselungsprogramm bereitgestellt, mit dem Dateien auf einem Speichergerät verschlüsselt werden können, wenn eine Verbindung zu einem Client mit dieser Einstellung erfolgt. Dateien werden beim Schreiben auf ein Speichergerät verschlüsselt und beim Lesen vom Gerät entschlüsselt. Ein Zugriff ist nur bei Angabe des korrekten Kennworts möglich – dem Kennwort, das bei der Erstellung eines verschlüsselten Ordners auf dem USB-Speichergerät definiert wird.

  WICHTIG: Erstellen Sie zunächst einen verschlüsselten Ordner auf dem USB-Gerät: Wenn ein Speichergerät für Dateiverschlüsselung konfiguriert wurde, müssen Benutzer zunächst mit dem Verschlüsselungsprogramm einen verschlüsselten Order erstellen (**Start > LANDesk Management > LANDesk Verschlüsselung > Erweitert > Verschlüsselten Ordner erstellen)**, bevor sie Dateien auf das Gerät kopieren können. Geben Sie bei der Erstellung eines verschlüsselten Ordners ein Kennwort ein. Wenn die Option "Kennworthinweise zulassen" aktiviert ist (siehe unten), hat der Benutzer die Möglichkeit, einen Hinweis als Merkhilfe für das Kennwort einzugeben. Die Eingabe eines Kennworthinweises ist jedoch nicht erforderlich.

- **Kein Zugriff:** Verhindert die Herstellung einer Verbindung zwischen Speichervolumes und einem Client, der mit dieser Einstellung für die Gerätesteuerung konfiguriert ist. Sie können Anpassungen hinsichtlich der Gerätetypen vornehmen, die dennoch zugelassen sind, indem Sie auf der Seite "Gerät" bestimmte Gerätetypen auswählen.

- **Ausnahmen:** Durch Klicken erstellen Sie Ausnahmen bezüglich der Zugriffsebene für Speichervolumes. Sie können Ausnahmen auf der Basis der Hardwarekennung, der Seriennummer des Mediums oder des Bustyps hinzufügen.
- **Verschlüsselungsoptionen:**
  - **Zugeordneter Speicherplatz für Verschlüsselung:** Gibt den Speicherplatz auf einem Plattenspeicherungsgerät an, der für verschlüsselte Dateien verwendet werden kann.
  - **Kennworthinweise zulassen:** Als Merkhilfe für das Kennwort des verschlüsselten Ordners kann der Endbenutzer hier einen Hinweis eingeben. Der Kennworthinweis darf nicht genau mit dem Kennwort übereinstimmen. Der Kennworthinweis darf maximal 99 Zeichen aufweisen. (Hinweis: Selbst wenn das Feld für die Eingabe eines Kennworthinweises zur Verfügung steht, muss der Benutzer keinen Hinweis eingeben.)
- **Endbenutzer benachrichtigen:** Zeigt ein Meldungsfeld an, wenn ein Benutzer eine Verbindung zu einem nicht autorisierten Plattenspeicherungsgerät herstellt. Weitere Informationen finden Sie unter "Hilfe zu den Einstellungen für die Gerätesteuerung" auf Seite 748.

Informationen über das Dialogfeld "Ausnahme konfigurieren" (für Speichervolumes)

Dieses Dialogfeld verwenden Sie, um eine Ausnahme bezüglich der Zugriffsebene für Speichervolumes zu erstellen.

- **Beschreibung:** Geben Sie eine Beschreibung ein, anhand derer diese Ausnahme identifiziert werden kann.
- **Parameter:** Wählen Sie den Parametertyp aus (Hardwarekennung, Seriennummer des Volumes oder Bustyp).
- **Wert:** Wenn der Parameter Hardwarekennung ausgewählt wurde, geben Sie eine Wertzeichenfolge ein.

- **Zugriff:** Gibt die Zugriffsebene für diese Ausnahme an (Voller Zugriff, Schreibgeschützter Zugriff, Nur verschlüsselt, Kein Zugriff).

Informationen zur Seite "Geräte"

Diese Seite verwenden Sie, um Optionen für diverse Gerätetypen zu definieren, die mit einem Client verbunden werden, der mit dieser Einstellung konfiguriert ist.

- **Geräte / Schnittstellen:** Verwenden Sie die Kontrollkästchen, um den Zugriff von Geräte und Schnittstellen auf den Client zu sperren.
- **Wireless LAN 802.11x sperren:** Sperrt eine Wireless-LAN802.11X-Verbindung.
- **Ausnahmen:** Klicken Sie hier, um Ausnahmen für gesperrte Geräte und Schnittstellen zu erstellen. Sie können Ausnahmen auf der Basis von Hardwarekennung, Klasse, Dienst, Enumerator, Anbieterkennung, Gerätekennung oder Gerätekennung des Anbieters hinzufügen.
- **CD/DVD-Laufwerke:** Legt die Zugriffsebene für CD/DVD-Laufwerke fest.
- **Ausnahmen:** Durch Klicken erstellen Sie Ausnahmen bezüglich der Zugriffsebene für CD/DVD-Laufwerke. Sie können Ausnahmen auf der Basis der Hardwarekennung, der Seriennummer des Mediums oder des Bustyps hinzufügen.
- **Endbenutzer benachrichtigen:** Zeigt ein Meldungsfeld an, wenn ein Benutzer eine Verbindung zu einem nicht autorisierten Plattenspeicherungsgerät herstellt.

Informationen über das Dialogfeld "Ausnahme konfigurieren" (für Geräte und Schnittstellen)

Dieses Dialogfeld verwenden Sie, um eine Ausnahme für gesperrte Geräte und Schnittstellen zu erstellen.

- **Beschreibung:** Geben Sie eine Beschreibung ein, anhand derer diese Ausnahme identifiziert werden kann.
- **Parameter:** Wählen Sie den Parametertyp aus (Hardwarekennung, Seriennummer des Volumes oder Bustyp).
- **Wert:** Wenn der Parameter Hardwarekennung ausgewählt wurde, geben Sie eine Wertzeichenfolge ein.
- **Zugriff:** Gibt die Zugriffsebene für diese Ausnahme an (Voller Zugriff, Schreibgeschützter Zugriff, Nur verschlüsselt, Kein Zugriff).

Informationen zur Seite "Schattenkopie"

Diese Seite verwenden Sie, um die Funktion "Schattenkopie" auf verwalteten Geräten, die mit dieser Einstellung konfiguriert wurden, zu aktivieren und konfigurieren.

Mit der Schattenkopie können Sie verfolgen, welche Dateien von dem bzw. auf das Gerät kopiert wurden, indem Sie eine duplizierte Kopie (eine "Schattenkopie") dieser Dateien in einem lokalen Verzeichnis erstellen.

- **Schattenkopie aktivieren:** Schaltet die Schattenkopie auf verwalteten Geräten ein, die mit dieser Einstellung konfiguriert wurden.
- **Nur Ereignisse protokollieren:** Gibt an, dass nur die Dateikopieraktivität in einer Protokolldatei aufgezeichnet wird, aber nicht die Dateien selbst, die kopiert werden.
- **Ausnahmen:** Klicken Sie, um Ausnahmen zu erstellen. Sie können Ausnahmen auf der Basis der Hardwarekennung, der Seriennummer des Mediums oder des Bustyps hinzufügen.
- **Lokaler Cache:** Gibt den Speicherort auf dem lokalen Laufwerk an, in dem die Schattenkopiedateien und die Protokolldatei gespeichert werden.

LANDesk Antivirus

LANDesk Antivirus – Übersicht

LANDesk Antivirus besteht aus einem integrierten Virenscanner-Agenten, einer Virensignaturdatenbank, die kontinuierlich aktualisiert wird, sowie Antivirus-Konfigurationsoptionen und -funktionen, die über das Extra **Agenteneinstellungen** bereitgestellt werden.

WICHTIG: Antivirus-Agent
Der Antivirus-Agent ist vom Agenten des Patch und Compliance-Sicherheitsscanners getrennt.

LANDesk Security Suite verwaltet eine aktuelle Datenbank mit Virendefinitions- und Musterdateien, die gedownloadet, bewertet und getestet sowie an Zielgeräte auf Ihrem Netzwerk verteilt werden können.

Sie können mit LANDesk Antivirus folgende Aktionen ausführen:

- Die neuesten Virendefinitions- und Musterdateien downloaden (die Antivirus-Signaturdatenbank des LANDesk Security Suite Dienstes wird mehrmals täglich aktualisiert).
- Einen Zeitplan für regelmäßige Virendefinitionsupdates aufstellen.
- Ältere Virendefinitionsdateien archivieren.
- Installationstasks des Antivirus-Agenten erstellen und verteilen.
- Antivirusscans auf den Zielgeräten automatisch und auf Abruf ausführen.
- Das Verhalten von Antivirusscans und Endbenutzeroptionen konfigurieren.
- Zu scannende Dateitypen auswählen und entscheiden, ob auf Riskware gescannt werden soll.
- Echtzeit-Virenschutz für Dateien und E-Mail aktivieren.
- Nach Antivirusscan-Engines anderer Hersteller scannen, Virenschutzscans in Echtzeit aktivieren/deaktivieren und sicherstellen, dass die Virenmusterdateien für diese spezifischen Antivirusprodukte auf dem neuesten Stand sind.
- Antivirusaktivität und Statusinformationen für die gescannten Geräte anzeigen.
- Antivirusalarme konfigurieren.
- Generieren von Antivirus-Berichten

Sicherheitsinhaltstypen und -abonnements

Wenn Sie LANDesk Management Suite oder LANDesk Security Suite installieren, umfasst die Installation standardmäßig das Extra "Patch und Compliance". Ohne Inhaltsabonnement für Security Suite können Sie jedoch nur auf LANDesk Softwareupdates und angepasste Definitionen scannen. Ein Security Suite Inhaltsabonnement gibt Ihnen die Möglichkeit, das Extra "Patch und Compliance" (und das Extra "Agenteneinstellungen") in vollem Umfang zu nutzen, da es Ihnen Zugriff auf zusätzliche Sicherheitsinhalte (Definitionstypen) gibt, einschließlich Erkennungsregeln für den Antivirusscanner und der eigentlichen LANDesk Antivirus-Virendefinitionsdateien, die der Antivirusscanner verwendet.

Folgende Typen von Sicherheitsinhalten gibt es:

- Antivirus-Updates (schließt für Scanner anderer Hersteller nur vom Antivirusscanner erkannten Inhalt ein; schließt im Falle von Antivirus sowohl vom Scanner erkannten Inhalt als auch Viren- sowie Riskware-Definitionsdateien ein, die in einer erweiterten Datenbank verfügbar sind)
- Blockierte Anwendungen (siehe "Rechtshinweis zum Typ "Blockierte Anwendung"" auf Seite 611)

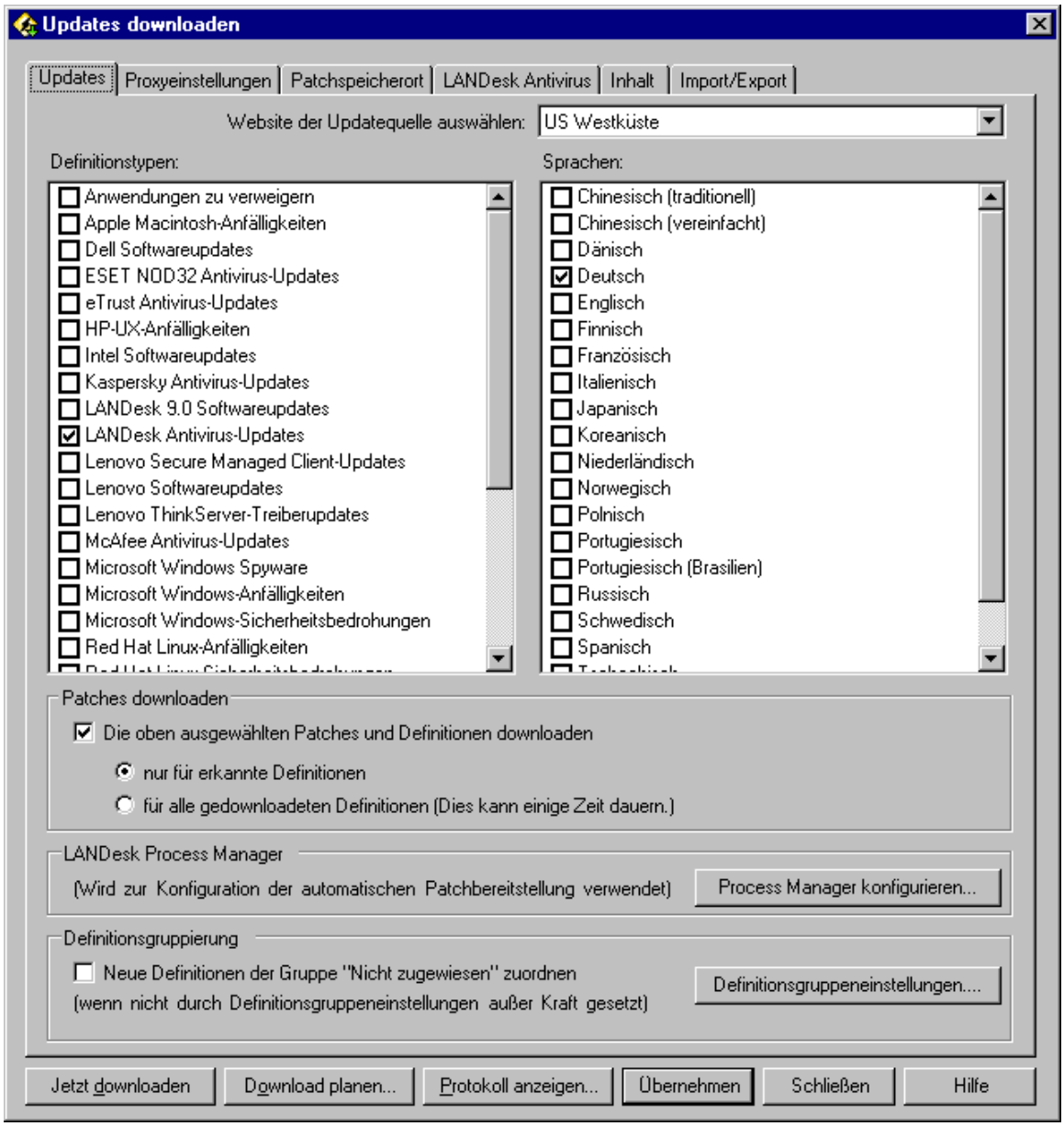
- Benutzerdefinierte Anfälligkeitsdefinitionen
- Treiberupdates
- LANDesk Softwareupdates
- Sicherheitsbedrohungen (Schwachstellen der Systemkonfiguration; umfasst Firewallerkennung und -konfiguration)
- Softwareupdates
- Spyware
- Anfälligkeiten (bekannte Plattformanfälligkeiten und anwendungsspezifische Anfälligkeiten)

Informationen zu den Security Suite-Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.

LANDesk Startseite

Verwenden von "Updates downloaden"

Bitte beachten Sie, dass die Liste der Definitionstypen auf der Seite **Updates** des Dialogfelds **Updates downloaden** mehrere Antivirus-Updates enthält, einschließlich eines Updates mit der Bezeichnung "LANDesk Antivirus-Updates". Wenn Sie LANDesk Antivirus-Updates auswählen, werden *sowohl* der vom Scanner erkannte Inhalt *als auch* die Updates der LANDesk Antivirus-Virendefinitionsdatei gedownloadet.



Für Scanner-Engines von Drittanbietern umfassen Antivirus-Updates Scannerdefinitionen, die Folgendes erkennen:

- Installation von gängigen Antivirusscanner-Engines (einschließlich des Extras "Antivirus")
- Scanstatus in Echtzeit (aktiviert oder deaktiviert)
- Scannerspezifische Musterdateiversionen (auf dem neuesten Stand oder veraltet)
- Datum des letzten Scans (ob der letzte Scan innerhalb des vom Administrator festgelegten maximal zulässigen Zeitraums erfolgte)

Im Falle des Antivirus-Scanners umfassen die Antivirus-Updates nicht nur den oben angegebenen Scanner-Erkennungsinhalt, sondern auch die vom Antivirus-Scanner verwendeten Virendefinitionsdateien.

HINWEIS: Vom Antivirus-Scanner erkannter Inhalt im Vergleich zu Virendefinitionsinhalt
Antivirus-Updates erstrecken sich nicht auf die eigentlichen Virendefinitions- oder Musterdateien. Wenn Sie Antivirus-Updates eines anderen Herstellers downloaden, wird nur von Scannern erkannter Inhalt in das Standardrepository gedownloadet, scannerspezifische Virendefinitionsdateien werden dagegen nicht gedownloadet. Wenn Sie jedoch Antivirus-Updates downloaden, werden *sowohl* vom Scanner erkannte Inhalte *als auch* die Antivirus-spezifischen Virendefinitionsdateien gedownloadet. Antivirus-Virendefinitionsdateien werden in einen separaten Speicherort auf dem Coreserver gedownloadet. Das Standardrepository für Virendefinitionsdateien ist der Ordner \LDLogon\Antivirus\Bases.

Unterstützte Geräteplattformen

Aktuelle Informationen zu den Clientplattformen, die Unterstützung für LANDesk Antivirus bieten, finden Sie im Dokument "OS Compatibility Feature Matrix" auf der Website der LANDesk Benutzercommunity:

LANDesk Benutzercommunity – Startseite

WICHTIG: Neustart erforderlich bei Windows NT 4.0-Geräten
Um den Antivirus-Dienst zu aktivieren, müssen Rechner, die unter Windows NT 4 laufen, nach der Bereitstellung der Agentenkonfiguration neu gestartet werden.

Sonstige Systemanforderungen

Achten Sie darauf, dass die verwalteten Geräte, die für den Antivirus-Agenten konfiguriert werden sollen, folgende Systemanforderungen erfüllen:

- Microsoft Internet Explorer 6.0 oder höher
- Es dürfen keine anderen Virenschutzprodukte installiert sein.

Rollenbasierte Administration mit LANDesk Antivirus

LANDesk Antivirus verwendet – genau wie Patch und Compliance – die rollenbasierte Administration, um Benutzern Zugriff auf Funktionen zu gewähren. Die rollenbasierte Administration ist das Zugriffs- und Sicherheitsmodell, mit dem Administratoren den Zugriff der Benutzer auf Extras und Geräte steuern. Jedem Benutzer werden bestimmte Rollen und Bereiche zugewiesen, die festlegen, mit welchen Funktionen dieser Benutzer arbeiten und welche Geräte er verwalten kann.

Der Administrator weist anderen Benutzern diese Rollen mithilfe des Extras "Benutzer" in der Konsole zu. Antivirus ist im Recht "Sicherheitskonfiguration" enthalten, das im Dialogfeld "Rollen" unter der Rechtegruppe "Sicherheit" erscheint. Damit ein Benutzer Antivirus-Funktionen anzeigen und verwenden kann, müssen ihm die hierfür erforderlichen Zugriffsrechte für Sicherheitskonfigurationen erteilt werden.

WICHTIG: Gruppenberechtigung "LANDesk Script Writers" erforderlich
Um geplante Tasks und Richtlinien im Extra "Patch und Compliance" und im Extra "Sicherheitskonfigurationen" (für Sicherheits- und Compliance-Scantasks, Reparaturtasks und Einstellungsänderungstasks) erstellen zu können, muss ein Benutzer über die Gruppenberechtigung "LANDesk Script Writers" verfügen. Mit anderen Worten: Der Benutzer muss einer Gruppe angehören, der die Berechtigung "LANDesk Script Writers" zugewiesen wurde. Weitere Informationen zur rollenbasierten Administration finden Sie unter "Benutzerverwaltung" auf Seite 40.

Mit dem Recht "Sicherheitskonfigurationen" können Benutzer Folgendes tun:

- Bereitstellen von Agentenkonfigurationen mit Antivirus auf Zielgeräten
- Download von Updates für Virendefinitionsdateien
- Geplante Updates erstellen
- Planen von Antivirus-Scantasks
- Antivirus-Einstellungen erstellen
- Antivirus-Scantasks und Einstellungsänderungs-Tasks für die Antivirus-Einstellungen bereitstellen
- Aktivieren von Datei- und E-Mail-Schutz in Echtzeit
- Konfigurieren von Antivirusscans für das Scannen nach bestimmten Dateitypen
- Ausschließen bestimmter Dateien, Ordner und Dateitypen (nach Erweiterung) von Antivirusscans
- Anzeigen von Antivirus-Scanaktivität und Statusinformationen für gescannte Geräte
- Aktivieren von Antivirusalarmen.
- Generieren von Antivirus-Berichten (erfordert zusätzlich Rollen für Berichte)

Antivirus-Task-Workflow

In den folgenden Schritten wird in groben Zügen beschrieben, welche Prozesse und Tasks bei der Implementierung eines Virenschutzes in Ihrem Netzwerk mit LANDesk Antivirus ablaufen. Jedes dieser Verfahren wird in den folgenden Abschnitten im Detail beschrieben.

Grundlegende Schritte zur Implementierung und Verwendung von LANDesk Antivirus

1. Konfigurieren von verwalteten Geräten für Antivirusscans.
2. Download von Updates für Virendefinitionen/Musterdateidefinitionen von einem Sicherheitsinhaltsserver.
3. Festlegen, ob Virendefinitionsdateien sofort auf den verwalteten Geräten installiert oder erst in einem Pilottest bewertet werden sollen.
4. Erstellen von Richtlinien und Antivirus-Scantasks, die entweder geplant oder auf Abruf ("on-demand") ausgeführt werden.
5. Konfigurieren von Antivirus-Einstellungen, die den Scanvorgang und die Endbenutzeroptionen bestimmen.
6. Scannen von verwalteten Geräten auf bekannte Viren und verdächtige Dateien.
7. Anzeigen der Ergebnisse eines Antivirusscans für gescannte Geräte.
8. Konfigurieren von Antivirusalarmen.
9. Generieren von Antivirus-Berichten.

Konfigurieren von Geräten für Antivirusschutz

Bevor verwaltete Geräte auf Viren gescannt und von Viren befreit werden können, muss der Antivirus-Agent auf dem Gerät installiert werden. Dies kann entweder bei der ursprünglichen Agentenkonfiguration für das Gerät geschehen oder im Rahmen eines separaten Installations- oder Updatetasks.

Überlegungen zur Bereitstellung von Antivirus

Wenn Sie Antivirus auf einem Gerät bereitstellen, auf dem bereits eine andere Virenschutzlösung installiert ist und läuft, aktiviert Antivirus seine Echtzeitschutzfunktion nicht, um mögliche Softwarekonflikte zu vermeiden. Sobald das andere Virenschutzprogramm entfernt wurde, kann die Echtzeit-Virenschutzfunktion von Antivirus aktiviert werden.

Sie haben die Möglichkeit, vorhandene Antivirus-Software während der LANDesk Antivirus-Bereitstellung automatisch von Zielgeräten entfernen zu lassen. Der Vorgang kann entweder beim erstmaligen Konfigurieren eines Agenten oder im Rahmen eines separaten Antivirus-Installations- oder Updatetasks durchgeführt werden. Antivirusprodukte, die von Geräten entfernt werden können, finden Sie unter "Liste der Antivirusprodukte von Drittanbietern, die automatisch entfernt werden können" auf Seite 756.

WICHTIG: Kennwort für Antivirus-Software löschen
Wenn ein vorhandenes Antivirus-Softwareprodukt mit einem Kennwort geschützt ist, müssen Sie erst das Kennwort löschen, da LANDesk Antivirus die Software andernfalls nicht deinstallieren kann.

Liste der Antivirusprodukte von Drittanbietern, die automatisch entfernt werden können

Antivirusprodukte, die während der Bereitstellung (oder Aktualisierung) von LANDesk Antivirus automatisch entfernt werden können:

- Symantec Antivirus (Versionen 7, 8, 9, 10)
- Symantec Endpoint Protection 11
- McAfee Enterprise (Versionen 7.0, 8.0i, 8.5)
- McAfee ePolicy Orchestrator EPO
- Trend Micro PC-cillin (Versionen 2004, 2005, 2006, 2007 15.3 unter Windows Vista 64-Bit)
- Trend Micro OfficeScan
- Trend Micro ServerProtect
- Trend Micro Internet Security 2008
- CA eTrust Antivirus (Versionen 6, 7.x, 8, 8.1)

Konfigurieren von Geräten für Antivirusschutz

So werden Geräte mit Antivirus über eine Agentenkonfiguration konfiguriert

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie in der Symbolleistenschaltfläche auf **Neues Windows**.
3. Wenn Sie die gewünschten Einstellungen für die Agentenkonfiguration eingegeben haben, müssen Sie zuerst auf der **Startseite** die Option **LANDesk Antivirus** wählen. Jetzt erhalten Sie Zugriff auf die Optionen der **LANDesk Antivirus**-Seite.
4. Klicken Sie auf die Gruppe **Sicherheit und Compliance** und klicken Sie dann auf **LANDesk Antivirus**.
5. Wenn Sie ein vorhandenes Antivirusprodukt von Zielgeräten entfernen möchten, wählen Sie die Option **Vorhandenes Antivirusprodukt entfernen** aus. Eine Liste mit den Antivirusprodukten, die von Geräten entfernt werden können, finden Sie unter "Liste der Antivirusprodukte von Drittanbietern, die automatisch entfernt werden können" auf Seite 756.

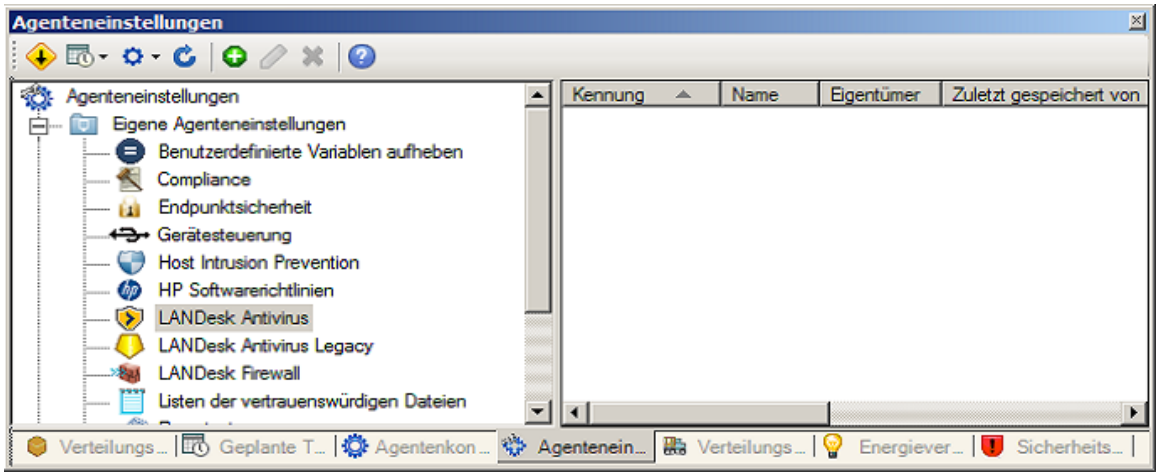
6. Wählen Sie eine Antivirus-Einstellung aus der verfügbaren Liste aus, um sie der von Ihnen erstellten Agentenkonfiguration zuzuweisen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Mithilfe der Antivirus-Einstellungen können Sie die Anzeige des Antivirus-Symbols in der Symbolleiste des Geräts ein- oder ausschalten, die Verfügbarkeit von interaktiven Optionen für Endanwender steuern, die Einstellungen in Bezug auf die Aktivierung von E-Mail-Scans und Echtzeitschutz festlegen, die zu scannenden Dateitypen und auszuschließenden Dateien und Ordner auswählen, infizierte Dateien unter Quarantäne stellen, Backups veranlassen und die Durchführung geplanter Antivirusscans und Virendefinitionsdateiupdates konfigurieren.
7. Legen Sie alle gewünschten Einstellungen für die Agentenkonfiguration fest und klicken Sie dann auf **Speichern**.

Sie können Geräte auch mit dem Extra "Sicherheitskonfigurationen" für Antivirus konfigurieren.

Verwendung des Extras "Sicherheitskonfigurationen"

Wenn Sie Antivirus zu einem späteren Zeitpunkt installieren oder aktualisieren möchten, können Sie dies mithilfe eines separaten Tasks von der Konsole aus tun.

Das Extra "Sicherheitskonfigurationen" (**Extras > Sicherheit > Sicherheitskonfigurationen**) verwenden Sie zur Installation oder Aktualisierung von Tasks, zum Entfernen von Tasks, für Antivirus-Definitionsdateiupdates und Scantasks.



So wird Antivirus als separater Task installiert oder aktualisiert

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Sicherheitskonfigurationen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten installieren oder aktualisieren**.
3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.
5. Wählen Sie die Komponente aus, die Sie installieren möchten. In diesem Falle wählen Sie LANDesk Antivirus. Sie können eine Antivirus-Einstellung aus der Liste der verfügbaren Einstellungen auswählen, um sie auf den von Ihnen erstellten Task anzuwenden. Sie können auch neue Einstellungen erstellen oder vorhandene Antivirus-Einstellungen bearbeiten.

6. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster des Zielgeräts anzeigen möchten, aktivieren Sie die Option **Fortschrittsdialog auf dem Client anzeigen**.
7. Wenn Sie ein vorhandenes Antivirusprodukt von Zielgeräten entfernen möchten, wählen Sie die Option **Vorhandenes Antivirusprodukt entfernen** aus. Eine Liste mit den Antivirusprodukten, die von Geräten entfernt werden können, finden Sie unter "Liste der Antivirusprodukte von Drittanbietern, die automatisch entfernt werden können" auf Seite 756.
8. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste der verfügbaren Einstellungen aus, um deren Neustartkonfiguration auf den Task anzuwenden, die Sie gerade erstellen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Der Task verwendet *ausschließlich* die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten während der Installation des Antivirus-Agenten.
9. Klicken Sie auf **OK**.

Entfernen von LANDesk Antivirus auf Geräten

Wenn Sie Antivirus auf verwalteten Geräten entfernen möchten, können Sie hierfür ebenfalls einen separaten Task verwenden.

So entfernen Sie LANDesk Antivirus

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Sicherheitskonfigurationen**.
2. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Sicherheitskomponenten entfernen**.
3. Geben Sie einen Namen für den Task ein.
4. Geben Sie an, ob die Installation ein geplanter Task, ein richtlinienbasierter Task oder beides ist.
5. Wenn Sie den Installationsverlauf im Sicherheitsscanner-Dialogfenster von Zielgeräten anzeigen möchten, wählen Sie die Option **Fortschrittsdialog auf dem Client anzeigen** aus.
6. Wählen Sie eine Scan- und Reparatureinstellung aus der Liste der verfügbaren Einstellungen aus, um deren Neustartkonfiguration auf den Task anzuwenden, die Sie gerade erstellen. Sie können neue Einstellungen erstellen oder vorhandene Einstellungen bearbeiten, indem Sie auf **Konfigurieren** klicken. Der Task verwendet *ausschließlich* die Neustartoptionen der ausgewählten Scan- und Reparatureinstellungen; diese bestimmen die Neustartanforderungen und -aktionen auf Zielgeräten beim Entfernen des Antivirus-Agenten.
7. Klicken Sie auf **OK**.

Virendefinitionsdateien aktualisieren

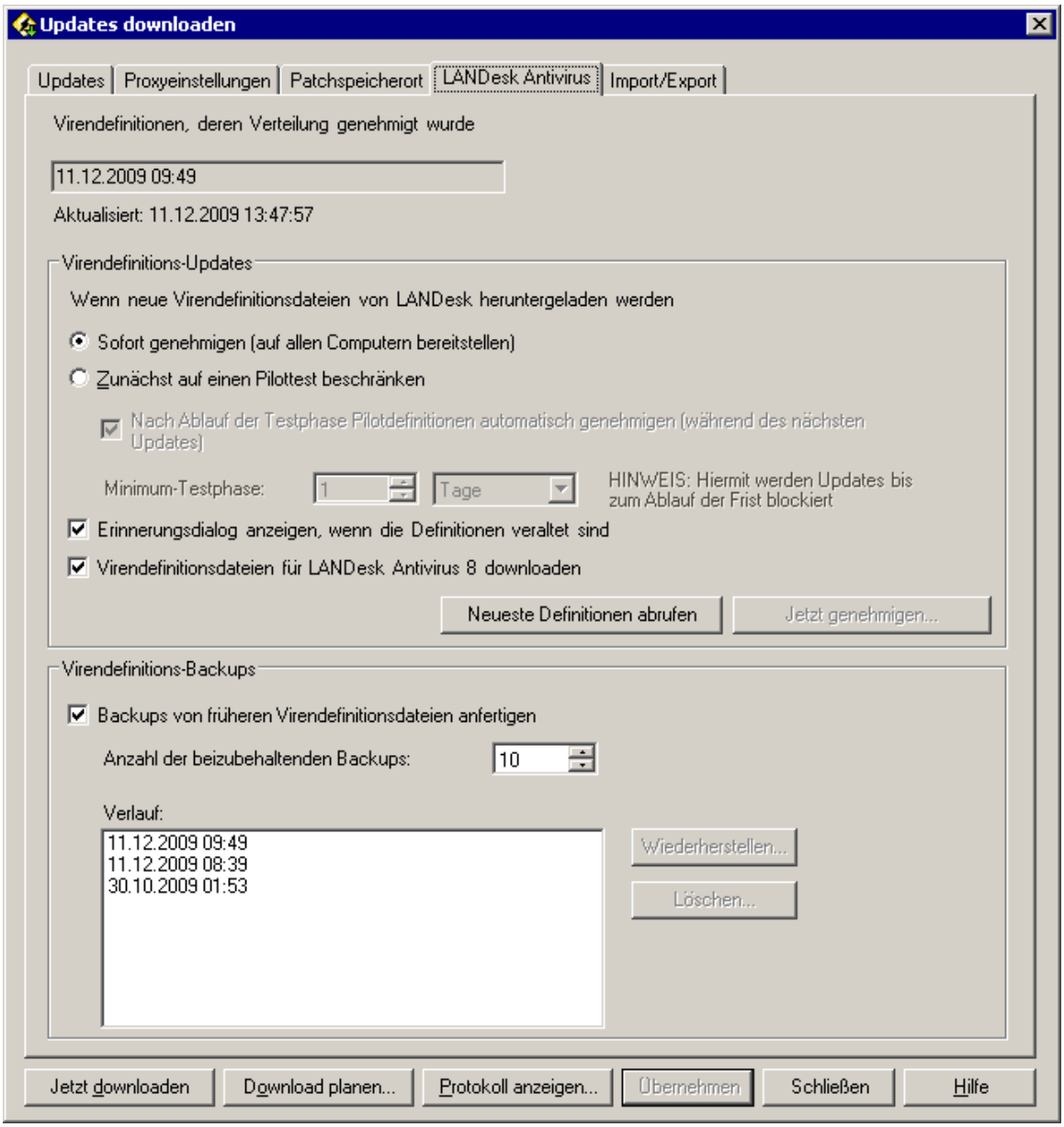
Mit Antivirus können Sie die aktuellsten Virendefinitionsdateien von den LANDesk Security Suite Inhaltsservern herunterladen. Die Virensignatur-Datenbank wird mehrmals täglich aktualisiert. Dadurch sind Ihre Virendefinitionen immer auf dem allerneuesten Stand, und Ihre verwalteten Geräte sind optimal vor neuen Bedrohungen geschützt.

Sie können die Virendefinitionsdateien von der Konsole aus entweder sofort als einmaligen Task oder als regelmäßig geplanten Task aktualisieren.

Verwenden von "Updates downloaden" für Virendefinitionsdateien

Sie verwenden "Updates downloaden" (**Sicherheitskonfigurationen > Updates downloaden**) um anzugeben, wohin Definitionsdateien kopiert werden sollen. Sie können im Standardspeicherort für Virendefinitionsdateien abgelegt und von dort aus für Zielgeräte bereitgestellt werden oder aber in einem Pilottest-Ordner, von wo aus sie zu Testzwecken vor der allgemeinen Bereitstellung nur an bestimmte Geräte verteilt werden.

Sie können bei der Erstellung eines Antivirus-Tasks direkt auf dieses Dialogfeld zugreifen.



HINWEIS: Verteilung von Virendefinitionsdateien an Endbenutzergeräte
Die heruntergeladenen Updates für Virendefinitionen können über Remotezugriff vom Coreserver aus

verteilt werden. Der Benutzer kann die Virendefinitionsdateien jedoch auch von seinem eigenen Rechner aus aktualisieren. Standardmäßig werden dazu die Dateien vom LANDesk Coreserver heruntergeladen. Wenn die aktuellsten Virendefinitionen jedoch heruntergeladen werden müssen, wenn der Benutzer nicht mit dem Netzwerk verbunden ist (z. B. auf Reisen oder wenn er einen Laptop verwendet), hat er die Möglichkeit, Dateien direkt vom LANDesk Security Suite Security-Inhaltsserver über einen Internetanschluss herunterzuladen.

So werden Updates für die Virendefinitionsdateien heruntergeladen

1. Klicken Sie auf **Extras > Sicherheit > Sicherheitskonfigurationen**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Updates downloaden**. Das Dialogfeld wird geöffnet und zeigt die Seite **Antivirus** an. (Sie können auch vom Extra "Patch und Compliance" aus auf das Dialogfeld **Updates downloaden** zugreifen.)
3. Wählen Sie auf der Seite **Updates** die Website in der Liste der verfügbaren Inhaltsserver aus, die als Quelle für die Updates dienen soll. Wählen Sie die Ihrem Standort nächstgelegene Quelle.
4. Wählen Sie auf der Seite **Updates** den Eintrag **Antivirus-Updates** aus der Liste **Definitionstypen** aus. (Sie können mehr als einen Definitionstyp pro Download auswählen. Sie brauchen jedoch einen Definitionstyp, der Ihrem LANDesk Security Suite Inhaltsabonnement entspricht. Je mehr Typen Sie auswählen, umso länger dauert die Aktualisierung.)
5. Wählen Sie auf der Seite **Updates** die Sprachen aus, deren Inhalt Sie für die von Ihnen angegebenen Typen aktualisieren möchten.
6. Wenn Sie veranlassen möchten, dass neuer Inhalt (d. h. Inhalt, der noch nicht in einer der Gruppen im Baum existiert) automatisch in die Gruppe "Nicht zugewiesen" eingefügt wird, anstatt in den Standardspeicherort (die Gruppe "Scannen"), aktivieren Sie das Kontrollkästchen **Neue Definitionen in die Gruppe "Nicht zugewiesen" einfügen**.
7. Klicken Sie jetzt auf **LANDesk Antivirus**, um den aktuellen Status der Virendefinitionsdateien anzuzeigen und spezifische Einstellungen für die Updates von Virendefinitionsdateien zu konfigurieren.
8. Klicken Sie auf **Sofort genehmigen**, wenn die Definitionen in den Standardordner (\LDLogon\Antivirus\Bases) auf dem Coreserver heruntergeladen werden sollen, von wo aus sie auf den Zielgeräten bereitgestellt werden können. Wenn Sie jedoch die Virendefinitionsdateien vor der Bereitstellung für Ihre verwalteten Geräte evaluieren möchten, klicken Sie auf **Zunächst auf einen Pilottest beschränken**. (Sie können auch einen Zeitraum angeben, nach dem die Dateien automatisch genehmigt werden, und eine Minimum-Testphase damit Sie dies nicht von Hand nach jedem Test tun müssen). Wenn Sie zuerst einen Pilottest durchführen, werden die Definitionsdateien in einen Pilottest-Ordner heruntergeladen und nur auf den Geräten bereitgestellt, die so eingestellt sind, dass sie die Pilotversion der Definitionsdateien erhalten.
9. Wenn auf der Coreserverkonsole eine Popupmeldung angezeigt werden soll, wenn die Virendefinitionsdateien in den vergangenen sieben Tagen nicht aktualisiert wurden, klicken Sie auf **Erinnerungsdialog anzeigen, wenn die Definitionen veraltet sind**.
10. Wenn Sie die aktuellsten Definitionsdateien sofort herunterladen möchten, klicken Sie auf **Neueste Definitionen abrufen**. Das Dialogfeld **Definitionen werden aktualisiert** zeigt den aktuellen Vorgang und Status an.
11. Wenn Sie die derzeit im Pilottest-Ordner befindlichen Virendefinitionen genehmigen möchten, klicken Sie auf **Jetzt genehmigen**. Dadurch werden die Definitionsdateien vom Pilottest-Ordner in den Standardordner (\LDLogon\Antivirus\Bases) verschoben.

12. Wenn Sie eine Sicherungskopie der Virendefinitionsdateien speichern möchten, die derzeit im Ordner "Bases" vorliegen, wählen Sie die Option **Backups anfertigen** aus. Die Backups der Definitionsdateien können jederzeit wiederhergestellt werden. Diese Sicherungskopien sind hilfreich, wenn Sie eine ältere Version der Virendefinitionsdatei erneut verwenden möchten. (Sicherungskopien der Virendefinitionsdateien werden in separaten Ordnern, und zwar nach dem Datum und der Uhrzeit ihrer Erstellung benannt, im Verzeichnis \LDLogon\Antivirus\Backups\ gespeichert.)
13. Klicken Sie auf **Jetzt downloaden**, um die Updates für den ausgewählten Sicherheitsinhalt herunterzuladen. Das Dialogfeld **Definitionen werden aktualisiert** zeigt den aktuellen Vorgang und Status an. Sie können aber auch auf die Schaltfläche **Download planen** klicken, um einen geplanten Task zu erstellen (siehe unten).
14. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Schließen**. Wenn Sie auf **Abbrechen** klicken, bevor die Aktualisierung abgeschlossen ist, werden nur die bis zu diesem Zeitpunkt verarbeiteten Sicherheitsinhalte in die Coredatenbank heruntergeladen. Sie müssen die Aktualisierung erneut ausführen, um den restlichen Sicherheitsinhalt abzurufen.

WICHTIG: Bei jedem Update für Virendefinitionsdateien auf verwalteten Geräten wird ein Miniscan der Speicherprozesse auf dem Gerät ausgeführt. Mit diesem Scan wird sichergestellt, dass die während des Updates im Speicher laufenden Prozesse nach wie vor virenfrei sind.

Einen Zeitplan für automatische Virendefinitionsdateiupdates aufstellen

Sie können Updates für Virendefinitionsdateien auch als geplante Tasks konfigurieren, die zu einem bestimmten Zeitpunkt in der Zukunft oder als wiederkehrende Tasks ausgeführt werden.

Konfigurieren Sie hierzu die Downloadoptionen für Sicherheitsinhalte im Dialogfeld **Updates downloaden** und wählen Sie "LANDesk Antivirus-Updates" in der Liste der Definitionstypen auf der Registerkarte **Updates**, konfigurieren Sie die Optionen für Virendefinitionsdateien auf der Registerkarte **LANDesk Antivirus** und klicken Sie dann auf die Schaltfläche **Update planen**. Das Dialogfeld **Informationen zum geplanten Update** zeigt taskspezifische Einstellungen für den Task an. Geben Sie einen Namen für den Task ein und klicken Sie auf **OK**, um einen Task der Kategorie "Sicherheitsinhalt downloaden" im Fenster "Geplante Tasks" zu erstellen, in dem Sie die Zeitplanoptionen festlegen können.

HINWEIS: Taskspezifische Einstellungen und globale Einstellungen
Beachten Sie, dass nur die Definitionstyp-, Sprach- sowie Definitions- und Patch-Downloadeinstellungen gespeichert und mit einem spezifischen Task während dessen Erstellung verknüpft werden. Diese drei Einstellungen gelten als taskspezifisch. Alle anderen Einstellungen auf den anderen Seiten des Dialogfeldes **Updates downloaden** sind global, d. h., sie gelten für alle nachfolgenden Downloadtasks für Sicherheitsinhalte. Die globalen Einstellungen umfassen: Patchdownload-Speicherort, Proxyserver, Spyware-Autofix, Sicherheitsalarme und Antivirus. Jedes Mal, wenn Sie eine globale Einstellung ändern, gilt diese Änderung für alle Sicherheitsinhalt-Downloadtasks von diesem Punkt an.

Prüfen der Virendefinitionsdateien mit einem Pilottest

Es ist manchmal sinnvoll, die Virendefinitionsdateien zuerst zu testen, bevor sie auf allen verwalteten Geräte bereitgestellt werden. Hierzu müssen Sie lediglich die Updates der Virendefinitionsdatei auf einen Pilottest-Ordner beschränken und dann Antivirus-Einstellungen anwenden, bei denen die Option **Pilotversion von Virenschutz-Definitionsdateien downloaden** ausgewählt ist.

So wird ein Pilottest der Virendefinitionsdateien ausgeführt.

1. Klicken Sie auf der Registerkarte **LANDesk Antivirus** des Dialogfensters **Update downloaden** auf **Zunächst auf einen Pilottest beschränken**.
2. Wenn Sie die getesteten Virendefinitionsdateien nicht manuell aus dem Pilottest-Ordner in den Standardordner (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8) verschieben möchten, klicken Sie auf **Genehmigung planen**, um einen geplanten Task zu erstellen, der einen Zeitpunkt für die Genehmigung der Pilottestdateien festlegt. Füllen Sie die Felder zu dem Task aus, der im Extra "Geplante Tasks" angezeigt wird. Wenn der festgelegten Zeitpunkt erreicht ist, werden die Virendefinitionsdateien automatisch genehmigt und verschoben.
3. Klicken Sie auf **Neueste Definitionen abrufen**, um die aktuellsten Virendefinitionsdateien vom LANDesk Security Suite Sicherheitsinhaltsserver herunterzuladen.
4. Um die derzeit im Pilottest-Ordner befindlichen Virendefinitionen sofort zu genehmigen, klicken Sie auf **Jetzt genehmigen**. Dadurch werden die Virendefinitionsdateien vom Pilottest-Ordner in den Standardordner (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8) verschoben.
5. Erstellen Sie daraufhin eine Antivirus-Einstellung für den Pilottest, mit der Virendefinitionsdateien für eine begrenzte Anzahl von Testrechnern bereitgestellt werden. Wählen Sie auf der Seite **Virendefinitionsupdates** die Option **Pilotversion von Virenschutz-Definitionsdateien downloaden**.
6. Wenden Sie die Antivirus-Einstellungen für den Pilottest auf einen Antivirus-Scantask für die ausgewählten Testcomputer an. Nun können Sie die Antivirusscan-Aktivitäten und Ergebnisse auf diesen Computern beobachten, um die Wirksamkeit der gedownloadeten Virendefinitionsdateien zu beurteilen, bevor diese an andere Geräte verteilt werden.

Sichern der Virendefinitionsdateien

Wenn Sie ältere Versionen gedownloadeter Virendefinitionsdateien sichern möchten, verwenden Sie hierzu die Einstellungen für **Virendefinitions-Backups** auf der Registerkarte **LANDesk Antivirus**.

Sicherungskopien von Virendefinitionsdateien können nützlich sein, wenn Sie auf eine ältere Definitionsdatei zurückgreifen müssen, um infizierte Dateien zu scannen, von Viren zu befreien oder eine Virendefinitionsdatei wiederherzustellen, mit der ein bestimmtes Problem beseitigt werden konnte.

Sicherungskopien der Virendefinitionsdateien werden in separaten Ordnern (nach dem Datum und der Uhrzeit ihrer Speicherung benannt) in folgendem Verzeichnis gespeichert: \LDLogon\Antivirus\Backups\.

Scannen von Geräten auf Viren

In diesem Abschnitt wird beschrieben, wie verwaltete Geräte auf bekannte Viren und verdächtige Objekte gescannt werden.

WICHTIG: Für das Scannen ist ein entsprechendes Inhaltsabonnement erforderlich
Vergessen Sie nicht, dass Sie zum Scannen auf bestimmte Sicherheitsinhaltstypen (einschließlich Viren) das entsprechende LANDesk Security Suite Inhaltsabonnement benötigen. Informationen zu den Inhaltsabonnements erhalten Sie von Ihrem LANDesk Händler; oder besuchen Sie die Website von LANDesk.
LANDesk Startseite

Scanmethoden

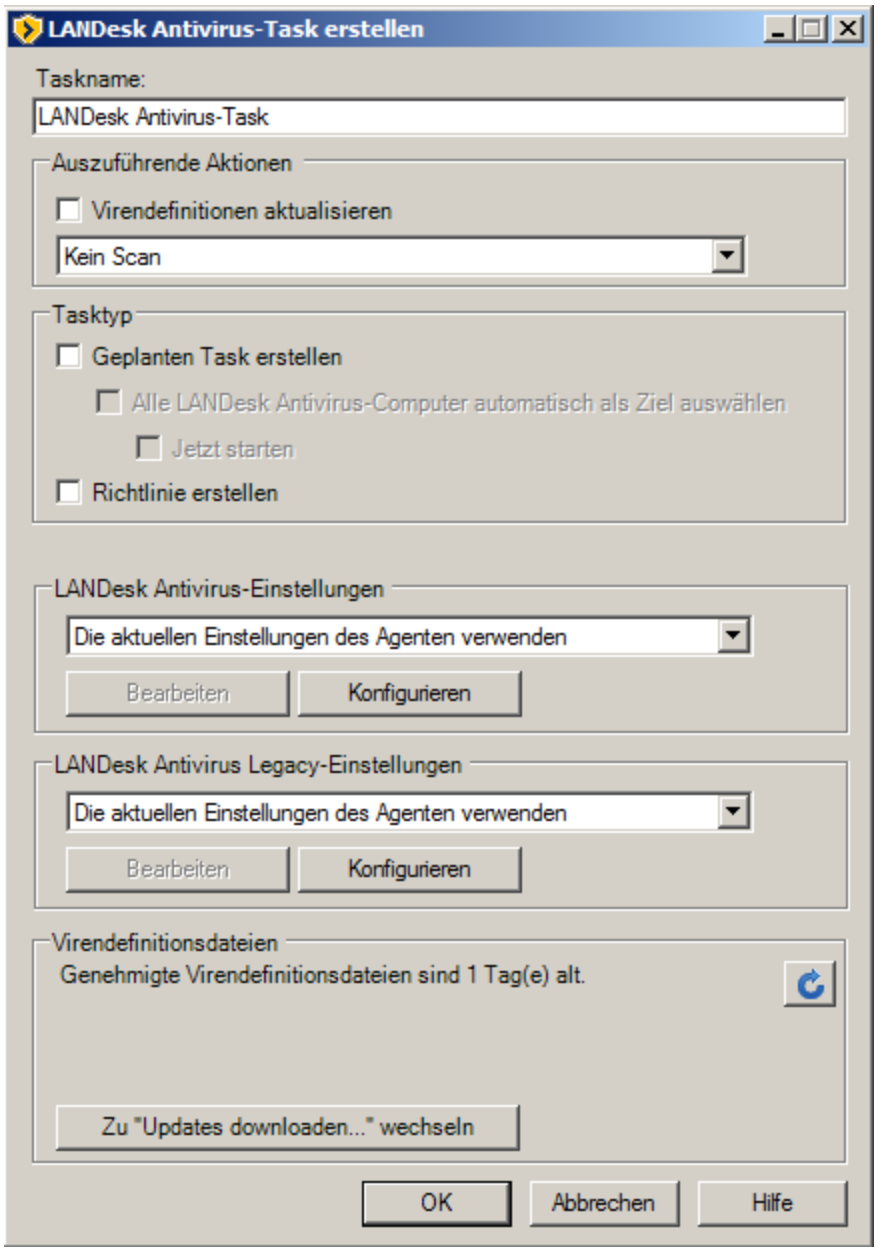
Für Antivirusscans auf verwalteten Geräten, auf denen Antivirus installiert ist, gibt es mehrere Prüfmethoden:

- Geplanter Antivirusscan
- Antivirusscan auf Abruf ("on demand")
- Benutzerinitiierter Antivirusscan
- Echtzeit-Dateischutz
- Echtzeit-E-Mailschutz

Ausführen eines geplanten Antivirusscans von der Konsole

Von der Konsole aus können Sie Antivirus-Scantasks so konfigurieren, dass sie entweder auf Abruf oder als geplanter Task bzw. Richtlinie durchgeführt werden.

Die Reparatur mittels geplantem Task lässt sich mit einer Pushverteilung vergleichen, da das Patch vom Coreserver via Pushprozedur an Geräte übermittelt wird. Eine Richtlinie ist dagegen als Pullverteilung einzustufen, da der Richtlinienagent auf dem Gerät den Coreserver auf zutreffende Richtlinien durchsucht und das Patch dann mittels Pullprozedur vom Coreserver abruft.



So erstellen Sie einen Antivirus-Scantask

1. Klicken Sie auf **Extras > Sicherheit > Sicherheitskonfigurationen**.
2. Stellen Sie sicher, dass die Virendefinitionsdateien in jüngster Zeit aktualisiert wurden.
3. Vergewissern Sie sich, dass der Standardordner (\LDLogon\Antivirus\Bases) mit den Virendefinitionsdateien nur die Definitionen enthält, die Sie zum Scannen verwenden möchten.
4. Klicken Sie auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **LANDesk Antivirus**.
5. Geben Sie einen Namen für den Task ein.

6. Geben Sie an, ob dieser Task Virenschutzdefinitionen aktualisieren soll, einen Antivirusscan durchführen soll oder beides.
7. Geben Sie an, ob es sich bei dem Task um einen geplanten Task, einen richtlinienbasierten Scan oder beides handelt.
8. Wenn Sie *alle* verwalteten Geräte scannen möchten, auf denen der Antivirus-Agent installiert ist, wählen Sie einen geplanten Task und dann alle Geräte als Zielgeräte aus. Sie können den Antivirusscan auch sofort für alle Geräte ausführen.
9. Um sicherzustellen, dass für den Scan die aktuellsten Virendefinitionsdateien verwendet werden, wählen Sie die Option **Virenschutzdefinitionen aktualisieren** aus.
10. Wählen Sie eine Antivirus-Einstellung aus der Liste der verfügbaren Einstellungen aus (oder erstellen Sie eine benutzerdefinierte Einstellung für diesen Scan, indem Sie auf die Schaltfläche **Konfigurieren** klicken), um festzulegen, wie der Scanner auf Endbenutzergeräten ausgeführt wird. Wenn für den Antivirusscan die lokalen Antivirus-Einstellungen des Geräts (Standardeinstellungen) verwendet werden sollen, wählen Sie diese Option aus der Liste aus. Weitere Informationen zum Konfigurieren des Antivirus-Scans mit Antivirus-Einstellungen finden Sie unter "Informationen zum Dialogfeld "LANDesk Antivirus-Einstellungen"" auf Seite 781.
11. Klicken Sie auf **OK**. (Für einen typischen Scan, der als geplanter Task ausgeführt wird, klicken Sie auf **OK**. Jetzt können Sie Zielgeräte hinzufügen und die Zeitplanoptionen im Tool "Geplante Tasks" konfigurieren.)

Ausführen eines Antivirusscans auf Abruf von der Konsole

Sie können auch einen sofortigen Antivirusscan auf einem oder mehreren Zielgeräten veranlassen.

Klicken Sie hierzu mit der rechten Maustaste auf das ausgewählte Gerät (oder auf bis zu 20 gleichzeitig ausgewählte Geräte), klicken Sie auf **LANDesk Antivirus - Jetzt scannen**, wählen Sie Antivirus-Einstellungen aus, legen Sie fest, ob Virendefinitionsdateien vor dem Scannen zu aktualisieren sind, und klicken Sie dann auf **OK**.

Wenn Sie auf "OK" klicken, werden im Dialogfenster **Status angeforderter Aktionen** folgende Informationen angezeigt:

- Verlauf
- Ergebnisse
- Scan-Zeitinformationen

Ausführen eines Antivirusscans auf einem verwalteten Gerät

Wenn Sie die Antivirus-Einstellungen so konfiguriert haben, dass das Antivirus-Symbol in der Taskleiste des Geräts angezeigt wird, kann der Benutzer außerdem seine eigenen Antivirusscans auf Abruf ausführen.

Hierzu klicken Sie auf dem verwalteten Gerät auf das Taskleistensymbol **LANDesk Antivirus** und wählen dann **Meinen Computer scannen** aus. Oder klicken Sie im Antivirus-Dialogfeld auf **Meinen Computer scannen**.

Aktivieren des Echtzeit-Virenschutzes (Dateien, E-Mail)

Der Echtzeit-Virenschutz führt fortlaufend Hintergrundscans der angegebenen Dateien, Dateitypen, E-Mail-Nachrichten und E-Mail-Anhänge basierend auf den bekannten Virendefinitionen durch. Außerdem können Sie eine Echtzeit-Benachrichtigung aktivieren, mit der der Benutzer über infizierte Dateien informiert wird.

Echtzeit-Dateischutz, E-Mail-Scannen und die Benachrichtigung werden über die Antivirus-Einstellungen konfiguriert.

HINWEIS: LANDesk Antivirus-Taskleistensymbol
Bei aktiviertem Echtzeit-Virenschutz ist das LANDesk Antivirus-Taskleistensymbol (auf dem Gerät des Endbenutzers) gelb. Das Symbol ist grau, wenn der Echtzeitschutz ausgeschaltet ist.

Echtzeit-Dateischutz

Der Echtzeit-Dateischutz wird mit den Optionen auf der Seite **Echtzeitschutz** des Dialogfelds **Antivirus-Einstellungen** konfiguriert. Für detaillierte Informationen klicken Sie auf **Hilfe**.

Wenn der Echtzeitschutz aktiv ist, werden Dateien auf Viren gescannt, und zwar jedes Mal, wenn die Datei folgendes durchführt:

- Öffnen
- Schließen
- Zugriff
- Kopieren
- Speichern

Echtzeit-E-Mail-Scans

Echtzeit-E-Mail-Scans werden mit der Option **E-Mail-Scan aktivieren** auf der Seite **Allgemein** des Dialogfelds **Antivirus-Einstellungen** konfiguriert.

Der Echtzeit-E-Mailschutz scannt alle ankommenden und abgehenden Nachrichten automatisch. Antivirus prüft nicht nur den Text der Nachricht, sondern auch angehängten Nachrichtentext und Dateianhänge.

Der Echtzeit-E-Mailschutz von Antivirus unterstützt folgende Programme:

- Microsoft Outlook

Wenn der Echtzeit-E-Mailschutz läuft, werden Nachrichten und Anhänge

- beim Öffnen bzw. bei der Vorschau gescannt
- nicht gescannt, wenn sie ausgewählt sind.

Wenn eine infizierte E-Mail auf einem verwalteten Gerät gefunden wird, versucht Antivirus, den Virus zu beseitigen. Kann die E-Mail desinfiziert werden, informiert eine neue Kopfzeile im Nachrichtentext den Endbenutzer. Kann die infizierte E-Mail nicht bereinigt werden, wird der gesamte Nachrichtentext gelöscht und durch eine neue Kopfzeile ersetzt.

Wenn eine verdächtige E-Mail-Nachricht gefunden wird, wird der Nachrichtentext in Plain Text konvertiert und eine Kopfzeile eingefügt.

Außerdem wird ein Dialogfeld für den Endbenutzer mit folgendem Inhalt angezeigt:

- Dateipfad
- Dateiname
- Virusname
- Hinweis an den Endbenutzer, dass er den Netzwerkadministrator benachrichtigen soll

Echtzeitbenachrichtigung (für infizierte Dateien)

Endbenutzer werden benachrichtigt, wenn eine mit einem Virus infizierte Datei erkannt, unter Quarantäne gestellt, gelöscht, übersprungen oder von Viren befreit wird.

Die Echtzeitbenachrichtigung für infizierte Dateien wird mit den Optionen auf der Seite **Echtzeitschutz** des Dialogfelds **Antivirus-Einstellungen** konfiguriert.

Es wird ein Dialogfeld auf dem Endbenutzergerät mit folgendem Inhalt angezeigt:

- Dateipfad
- Dateiname
- Virusname
- Hinweis an den Endbenutzer, dass er den Netzwerkadministrator benachrichtigen soll

Konfigurieren der Antivirus-Scanoptionen mit Antivirus-Einstellungen

Mit Antivirus haben Sie die vollständige Kontrolle über die Ausführung von Antivirusscans auf Zielgeräten und darüber, welche Optionen dem Endbenutzer zur Verfügung stehen. So kann es zum Beispiel (je nach Zweck oder geplantem Zeitpunkt eines Antivirusscans) sinnvoll sein, den Antivirus-Client auf dem Endbenutzergerät anzuzeigen und dem Endbenutzer die Durchführung von Antivirusscans, das Anzeigen und Wiederherstellen von Objekten in Quarantäne, den eigenständigen Download von Virendefinitionsupdates usw. zu erlauben. Sie können dies tun, indem Sie Antivirus-Einstellungen erstellen und auf Scantasks anwenden.

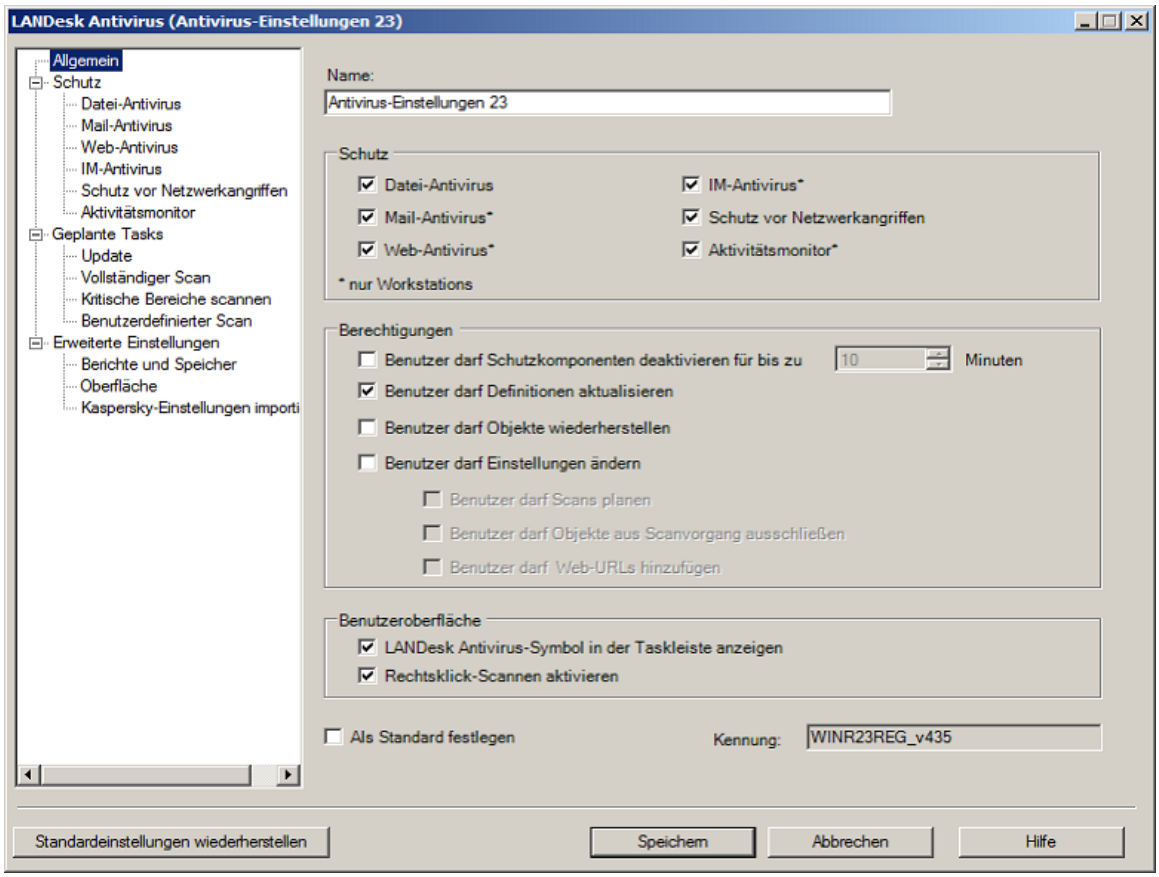
Über die Antivirus-Einstellungen können Sie folgende Optionen konfigurieren:

- Ob das Antivirus-Symbol in der Taskleiste angezeigt wird (wodurch Benutzern Zugriff auf Antivirusscans erteilt wird und sie die Möglichkeit erhalten, Quarantänebereiche und Backups anzuzeigen sowie Tasks zur Dateihandhabung auszuführen).
- Echtzeit-E-Mail-Scans
- Endbenutzer-Rechtsklick-Scans
- CPU-Nutzung
- Eigentümer (um den Zugriff zu beschränken)
- Geplante Antivirusscans
- Größe des Quarantäne-/Sicherungsordners
- Wiederherstellung infizierter und verdächtiger Objekte
- Angabe, welche Dateien, Ordner und Dateitypen gescannt werden sollen
- Scanausschlüsse
- Ob eine heuristische Analyse zur Erkennung verdächtiger Dateien eingesetzt werden soll
- Ob auf Riskware gescannt werden soll
- Echtzeit-Dateischutz (einschließlich welche Dateien gescannt werden sollen, Heuristik und Ausschlüsse)
- Downloaden von Updates für Virendefinitionsdateien (Pilottestversionen, geplante Downloads, Endbenutzerberechtigung zum Download und direkte Downloads vom Sicherheitsinhaltsserver)

Alle von Ihnen erstellten Antivirus-Einstellungen werden in der Gruppe **LANDesk Antivirus** im Extra **Sicherheitskonfigurationen** gespeichert.

Verwenden von Antivirus-Einstellungen

Sie können Antivirus-Einstellungen (ein gespeicherter Satz konfigurierter Optionen) erstellen und auf Scantasks anwenden. Sie können beliebig viele Antivirus-Einstellungen erstellen. Antivirus-Einstellungen können für einen bestimmten Zweck, Zeitpunkt oder Satz von Zielgeräten definiert werden.



So werden Antivirus-Einstellungen erstellt

1. Klicken Sie im Extra **Sicherheitskonfigurationen** mit der rechten Maustaste auf das Objekt **LANDesk Antivirus** und klicken Sie dann auf **Neu**. (Hinweis: Sie können auf dieses Dialogfeld auch zugreifen, indem Sie in einem beliebigen Taskdialog, in dem Sie Antivirus-Einstellungen übernehmen können, auf **Bearbeiten** oder **Konfigurieren** klicken.)
2. Geben Sie einen Namen für die Antivirus-Einstellungen ein.
3. Geben Sie die Einstellungen wie gewünscht auf den Seiten für den spezifischen Task ein. Für weitere Informationen zu einer Option klicken Sie auf **Hilfe**.

Nachdem Sie die Antivirus-Einstellungen konfiguriert haben, können Sie sie auf Antivirus-Tasks (oder auf Einstellungsänderungs-Tasks) anwenden.

Ändern der Antivirus-Standardeinstellungen für Geräte

Die Antivirus-Standardeinstellungen eines Geräts werden als Teil der ursprünglichen Agentenkonfiguration bereitgestellt. Wenn ein Task mit einer anderen Antivirus-Einstellung verknüpft ist oder ihm eine solche Einstellung zugewiesen wurde, werden die Standardeinstellungen überschrieben. Sie können die Standardeinstellung des Geräts verwenden, indem Sie sie beim Erstellen eines Tasks auswählen.

Es kann zu einem späteren Zeitpunkt sinnvoll sein, diese Antivirus-Standardeinstellungen auf bestimmten Geräten zu ändern. Patch und Compliance bietet eine Möglichkeit, diese Änderung vorzunehmen, ohne erneut eine komplett neue und vollständige Agentenkonfiguration bereitstellen zu müssen. Verwenden Sie hierfür den Task **Einstellungen ändern** in der Dropdownliste der Symbolleistenschaltfläche **Task erstellen**. In das eingeblendete Dialogfeld können Sie einen eindeutigen Namen für den Task eingeben, festlegen, ob es sich um einen geplanten Task oder eine Richtlinie handelt, und entweder vorhandene Einstellungen als Standard auswählen oder mithilfe der Schaltfläche "Bearbeiten" neue Einstellungen als Standard für Zielgeräte erstellen.

Anzeigen von Antivirus-Einstellungen im Inventar

Sie können Antivirus-Einstellungen in der Inventaransicht aufdecken und/oder überprüfen.

Klicken Sie hierzu mit der rechten Maustaste auf das ausgewählte Gerät und klicken Sie **Inventar > LANDesk Management > AV-Einstellungen**.

Konfigurieren der zu scannenden Dateien (nur infizierbare Dateien, Ausschlüsse, Heuristik, Riskware)

Sowohl für Antivirusscans als auch für den Echtzeit-Antivirus-Dateischutz können Sie angeben, welche Dateien (Elemente) Sie scannen möchten und welche nicht.

In diesen Abschnitten finden Sie weitere Informationen dazu, wie Sie festlegen können, welche Dateien/Elemente gescannt werden sollen.

- "Alle Dateien oder nur infizierte Dateien" auf Seite 769
- "Ausschluss von Objekten aus Antivirusscans und Echtzeitschutz" auf Seite 771
- "Verwendung heuristischer Analysen zum Scannen auf verdächtige Objekte" auf Seite 771
- "Scannen auf Riskware (erweiterte Datenbank)" auf Seite 772

Alle Dateien oder nur infizierte Dateien

Geben Sie auf den Seiten **Virenscan** und **Echtzeitschutz** der Antivirus-Einstellungen an, ob alle Dateien oder nur infizierbare Dateien gescannt werden sollen.

- **Alle Dateitypen scannen:** Legt fest, dass alle Dateitypen auf dem Zielgerät von einem Antivirusscan gescannt werden. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Es empfiehlt sich deshalb, alle Dateitypen mit einem Scan auf Abruf anstatt Echtzeitschutz zu scannen.
- **Nur infizierbare Dateien scannen:** Gibt an, dass nur infizierbare Dateien vom Scan zu prüfen sind. Als infizierbar gelten alle Dateien, die als virenanfällig bekannt sind. Das Scannen auf infizierbare Dateien zu begrenzen ist effizienter, als alle Dateien zu scannen, da einige Viren nur bestimmte Dateitypen infizieren. Sie sollten es sich jedoch zur Angewohnheit machen, alle Dateien in regelmäßigen Abständen mit On-Demand-Scans zu überprüfen, um sicherzustellen, dass die Geräte virenfrei sind.

Infizierbare Dateitypen

Infizierbare Dateitypen werden nicht anhand ihrer Dateierweiterung, sondern anhand ihrer Format-ID im Datei-Header identifiziert. Auf diese Weise wird sichergestellt, dass auch umbenannte Dateien gescannt werden.

Zu den infizierbaren Dateien zählen folgende: Dokumentdateien wie Word- und Excel-Dateien, mit Dokumentdateien verbundene Vorlagendateien und Programmdateien wie Dynamic Link Libraries (.DLLs), Kommunikationsdateien (.COM), ausführbare Dateien (.EXEs) sowie andere Programmdateien. Nachstehend finden Sie eine nach der Standard- oder Original-Dateierweiterung des Dateiformats sortierte Liste infizierbarer Dateitypen.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML
- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX

- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

Ausschluss von Objekten aus Antivirusscans und Echtzeitschutz

Sie können auch angeben, welche Objekte von Antivirusscans oder Echtzeit-Dateischutzscans ausgeschlossen werden sollen. Sie konfigurieren Ausschlüsse für Antivirusscans, indem Sie Dateien, Ordner und Dateitypen der Ausschlussliste auf den Seiten **Virenscan** und **Echtzeitschutz** für die jeweiligen Antivirus-Einstellungen hinzufügen.

HINWEIS: Die Liste "Vertrauenswürdige Elemente" auf verwalteten Geräten
Beachten Sie, dass Sie darüber hinaus auch eine Option aktivieren können, die es Benutzern ermöglicht, Dateien und Ordner anzugeben, die nicht von LANDesk Antivirus gescannt werden sollen. Diese Funktion wird über die Liste "Vertrauenswürdige Elemente " verwaltet, die auf der Seite **Allgemein** der Antivirus-Einstellungen konfiguriert wird.

Verwendung heuristischer Analysen zum Scannen auf verdächtige Objekte

Sie können können die heuristische Analyse aktivieren, um mit Antivirusscans und Echtzeit-Dateischutz nach verdächtigen (möglicherweise infizierten) Dateien zu suchen.

Geben Sie das Scannen mit der heuristische Analyse auf den Seiten **Virenscan** und **Echtzeitschutz** der Antivirus-Einstellungen an.

Mithilfe der heuristischen Analyse wird versucht, Dateien zu finden, die möglicherweise mit einem unbekannten (d. h. einem nicht in der Virensignaturdatenbank definierten) Virus infiziert sein könnten. Hierzu wird nach verdächtigem Verhalten gesucht. Verdächtiges Verhalten ist zum Beispiel, wenn ein Programm sich selbst modifiziert, sofort versucht, andere ausführbare Dateien zu finden oder geändert wird, nachdem es beendet wurde. Eine heuristische Analyse ahmt die Programmausführung nach, um Protokolle der beobachteten verdächtigen Aktivität zu erstellen. Sie verwendet dann diese Protokolle, um mögliche Vireninfektionen zu identifizieren. In fast allen Fällen ist dieser Mechanismus wirksam und zuverlässig, und er erzeugt nur selten falsche positive Ergebnisse.

Antivirus verwendet die heuristische Analyse zur Verifizierung von Dateien, die bereits mit einem Antivirusscan basierend auf den bekannten Virendefinitionen geprüft wurden.

Es ist zu beachten, dass heuristische Scanverfahren die Leistung auf verwalteten Geräten beeinträchtigen können.

Scannen auf Riskware (erweiterte Datenbank)

Antivirus gibt Ihnen die Möglichkeit, auf Zielgeräten nach riskanter Software, auch Riskware genannt, zu suchen. Riskante Software ist im Wesentlichen Clientsoftware, deren Installation ein mögliches, jedoch kein definitives Risiko für den Endbenutzer darstellt.

Beispiele für Riskware sind Adware, Proxyprogramme, Pornware, Remoteverwaltungsprogramme, IRC, Dialer, Aktivitätsmonitore, Kennwortprogramme und Internetprogramme wie FTP, Web, Proxy und Telnet.

Wenn Sie definieren, dass verwaltete Geräte auf riskante Software zu scannen sind, lädt Antivirus eine erweiterte Datenbank, in der sich Definitionsdateien befinden, die zur Ausführung des Scans verwendet werden. Der erweiterte Datenbankscan ist zeitaufwändiger als der standardmäßige Antivirusscan.

Zusätzliche Hinweise über Scandateien

- **Scannen der System-Restore-Points:** Antivirus scannt die Dateien in allen System-Restore-Point-Ordnern, die auf dem verwalteten Gerät vorhanden sind.

Was geschieht auf einem Gerät während eines Antivirusscans?

In diesem Abschnitt wird beschrieben, wie Antivirus auf Endbenutzergeräten mit installierter Antivirus-Software angezeigt wird und was geschieht, wenn Geräte von einem Antivirusscan oder dem Echtzeit-Virenschutz auf Viren überprüft werden. Mögliche Endbenutzeroptionen werden ebenso aufgeführt wie die Aktionen, die die Benutzer in die Wege leiten können, wenn der Scan ein infiziertes Objekt ausfindig macht.

Antivirus-Clientoberfläche und Endbenutzeraktionen

Wenn die Option **LANDesk Antivirus-Symbol in der Taskleiste anzeigen** in den Antivirus-Einstellungen des Geräts ausgewählt wurde, wird der Antivirus-Client, der folgende Elemente einblendet, angezeigt:

Taskleistensymbol

- Echtzeitschutz ist aktiviert (gelbes Taskleistensymbol) oder deaktiviert (graues Taskleistensymbol)

Antivirus-Fenster

- Der Echtzeitschutz ist aktiviert oder deaktiviert (wenn die Option in den Antivirus-Einstellungen aktiviert ist, kann der Endbenutzer den Echtzeitschutz maximal so lange deaktivieren, wie die von

Ihnen angegebene Zeitspanne zulässt)
- E-Mail-Scanning ist aktiviert oder deaktiviert
- Letzter Scan (Datum und Uhrzeit)
- Geplanter Scan (Datum und Uhrzeit)
- Versionsnummer der Scan-Engine
- Virendefinitionen (Zeitpunkt der letzten Aktualisierung der Musterdateien)
- Quarantäne (Zeigt die Anzahl der in Quarantäne befindlichen Objekte an.) Benutzer können auf **Details anzeigen** klicken, um das Dialogfeld "Unter Quarantäne gestellte Elemente" zu öffnen. Wenn die Option aktiviert ist, können Benutzer Dateien zudem auch wiederherstellen. Wenn der Kennwortschutz aktiviert ist, muss der Endbenutzer das Kennwort eingeben.)
- Sicherung (Anzahl der gesicherten Objekte)
- Vertrauenswürdige Elemente (zeigt an, welche Elemente der Endbenutzer seiner Liste der vertrauenswürdigen Elemente hinzugefügt hat, um zu verhindern, dass diese Elemente auf Viren oder riskante Software gescannt werden)

Endbenutzeraktionen

Wenn Antivirus auf dem Computer eines Endbenutzers installiert ist und die Antivirus-Einstellungen (Standard oder taskspezifisch) dies erlauben, kann der Benutzer folgende Tasks ausführen:

- Meinen Computer scannen (Scanstatus anzeigen und Scan anhalten und abbrechen)
- Mit der rechten Maustaste klicken, um Antivirusscans in Dateien und Ordnern in Windows Explorer durchzuführen (sofern die Option in der Antivirus-Einstellung aktiviert wurde)
- Lokale geplante Antivirus-Scantasks anzeigen
- Lokale geplante Antivirusscans auf eigenem Computer anzeigen (wenn die Option durch die Antivirus-Einstellung aktiviert wurde).
- Virendefinitionsdateien aktualisieren
- Den Echtzeitschutz vorübergehend deaktivieren (sofern die Option in der Agentenkonfiguration aktiviert wurde und auf einen bestimmten Zeitraum begrenzt)
- Unter Quarantäne gestellte Objekte anzeigen
- Sicherungsobjekte anzeigen
- Vertrauenswürdige Elemente anzeigen
- Verdächtige Objekte wiederherstellen (sofern diese Option in der Antivirus-Einstellung aktiviert wurde)
- Infizierte Objekte und riskante Software wiederherstellen (sofern diese Option in der Antivirus-Einstellung aktiviert wurde)
- Dateien und Order/Unterordner in die Liste der vertrauenswürdigen Elemente einfügen oder daraus entfernen

Beachten Sie, dass Endbenutzer weder Antivirusscan-Einstellungen konfigurieren noch E-Mail-Scans deaktivieren können.

Wenn ein infiziertes Objekt erkannt wird

Dieser Prozess kommt bei infizierten Dateien und E-Mail-Nachrichten zur Anwendung.

1. Das infizierte Objekt wird automatisch gesichert. (Die Sicherungsdatei wird im Ordner \LDClient\Antivirus\ mit der Erweiterung *.bak gespeichert.)
2. Es wird versucht, das infizierte Objekt vom Virus zu befreien.
3. Wenn der Virus entfernt werden kann, wird das Objekt an seinem ursprünglichen Speicherort wiederhergestellt.
4. Wenn der Virus nicht aus dem infizierten Objekt entfernt werden kann, wird das Objekt unter Quarantäne gestellt. (Der Viren-String wird entfernt und die Datei verschlüsselt, damit sie nicht ausgeführt werden kann. Die unter Quarantäne gestellte Datei wird im Ordner \LDClient\Antivirus\ mit der Erweiterung *.qar gespeichert.)

Wenn die entsprechende Option in seinen Antivirus-Einstellungen (Standard oder taskspezifisch) aktiviert ist, kann der Endbenutzer unter Quarantäne gestellte Objekte wiederherstellen, löschen und erneut scannen.

Automatisches Scannen von unter Quarantäne gestellten Dateien

Wenn ein Antivirusscan auf Abruf ausgeführt wird oder die Virendefinitionsdateien aktualisiert werden, scannt der Antivirus-Scanner automatisch die Objekte im Quarantäne-Ordner für den Fall, dass infizierte Dateien mit den aktuellsten Virendefinitionsdateien jetzt von Viren befreit werden können.

Wenn der Virus aus einer Datei im dem Quarantäne-Ordner entfernt werden kann, wird diese automatisch wiederhergestellt und der Benutzer informiert.

Der Endbenutzer kann eine gesicherte Datei öffnen und den Dateikopf einsehen, der Informationen zum ursprünglichen Speicherort der Datei sowie zum Grund für die Sicherung dieser Datei enthält.

Es ist zu beachten, dass nur der ursprüngliche Benutzer (d. h. der Benutzer, der zum Zeitpunkt der Erkennung der infizierten Daten eingeloggt war) Sicherungsdateien löschen oder ändern kann.

Antivirusalarme konfigurieren.

Sie können Antivirusalarme konfigurieren, damit Sie bei der Erkennung von bestimmten Virenausbrüchen auf verwalteten Geräten in Ihrem System benachrichtigt werden. Antivirus verwendet hierzu das Standard-Alarmtool von LANDesk.

Virenausbruchparameter werden auf der Basis der Anzahl der verwalteten Geräte definiert, die innerhalb eines bestimmten Zeitraums durch einen Virus infiziert werden.

So werden Antivirusalarme konfiguriert

Die Antivirus-Alarmeinstellungen sind auf der Seite **Antivirus** des Dialogfelds **Alarmeinstellungen** zu finden.

Sie müssen zuerst die Antivirusalarme im Extra "Alarmeinstellungen" der Konsole konfigurieren. Es gibt u. a. folgende Antivirusalarme:

- Eine Virenschutzaktion, für die ein Alarm generiert werden kann, ist fehlgeschlagen.
- Eine Virenschutzaktion, für die ein Alarm generiert werden kann, wurde erfolgreich ausgeführt.
- Virenausbruch-Alarm (pro Virus)

Folgende Antivirusereignisse können Antivirusalarme generieren:

- Virusentfernung fehlgeschlagen
- Virusentfernung erfolgreich

- Quarantäne fehlgeschlagen
- Quarantäne erfolgreich
- Löschen fehlgeschlagen
- Löschen erfolgreich

Wählen Sie die gewünschten Alarme aus. Mit der Option "Zeitraum" wird verhindert, dass zu häufig Alarme generiert werden. Wenn innerhalb des angegebenen Zeitraums (für einen beliebigen Antivirusauslöser) mehr als ein Alarm gegeben wird, werden alle Alarme nach dem ersten ignoriert.

Sie können den vollständigen Antivirus-Alarmverlauf in der Ansicht "Sicherheitsinformationen" des jeweiligen Geräts einsehen. Klicken Sie mit der rechten Maustaste auf ein Gerät, und wählen Sie "Sicherheitsinformationen" aus. Wählen Sie dann in der Dropdownliste "Typ" den Antivirustyp und schließlich das Objekt "Antivirus-Verlauf" aus.

Generieren von Antivirus-Berichten

Antivirus-Informationen werden in mehreren Berichten im Extra "Berichte" dargestellt. Diese Berichte bieten nützliche Informationen zur Antivirus-Scanaktivität und zum Status von gescannten Geräten in Ihrem Netzwerk.

Um auf das Extra "Berichte" zugreifen und Berichte generieren und anzeigen zu können, müssen Benutzer über das Recht "LANDesk Administrator" (d. h. uneingeschränkte Rechte) und die spezifischen Rollen für "Berichte" verfügen.

Weitere Informationen zur Verwendung des Extras "Berichte" finden Sie unter "Berichte" auf Seite 209.

Anzeigen von Antivirus-Informationen im Executive Dashboard

Informationen zum Antivirusscan können auch im Executive-Dashboard der LANDesk Webkonsole angezeigt werden. Diese Daten sind hilfreich zur Identifizierung von Virenausbrüchen und zur Anzeige des Virenschutzverlaufs.

LANDesk Antivirus-spezifische Widgets zeigen Folgendes an:

- Die Top-5-Viren (der letzten 10 Tage oder Wochen)
- Von Viren infizierte verwaltete Geräte (in den letzten 10 Tagen oder Wochen)
- Prozentsatz der verwalteten Geräte, bei denen der Echtzeitschutz aktiviert ist
- Prozentsatz der verwalteten Geräte, bei denen die Virendefinitionen auf dem letzten Stand sind

Hilfe zu LANDesk Antivirus

Der Zugriff auf die LANDesk Antivirusfunktionen erfolgt über das Fenster des Extras "Agenteneinstellungen" (**Extras > Sicherheit > Agenteneinstellungen**).

Mit Antivirus können Sie Antivirusinhalt (d. h. Virendefinitionsdateien) downloaden und verwalten, Antivirusscans konfigurieren und Anzeige-/Interaktionseinstellungen für den Antivirus-Scanner anpassen, mit denen festgelegt wird, wie der Scanner auf Zielgeräten angezeigt wird und arbeitet und welche interaktiven Optionen Endbenutzern zur Verfügung stehen. Außerdem können Sie auf den Virenschutz bezogene Informationen für gescannte Geräte anzeigen, Virenschutzalarmmeldungen aktivieren und Virenschutzberichte generieren.

Der Hauptabschnitt zu "LANDesk Antivirus" auf Seite 751 bietet eine Einführung zu diesem komplementären Sicherheitsverwaltungstool, das sowohl in LANDesk Management Suite als auch in LANDesk Security Suite enthalten ist. Im vorliegenden Abschnitt finden Sie einen Überblick, Informationen zum Abonnement von Antivirusinhalt sowie Schrittanleitungen zur Verwendung der Antivirusfunktionen.

Dieser Abschnitt enthält die nachstehend genannten Hilfethemen, in denen die Dialogfelder von Antivirus beschrieben werden. Von der Konsolenoberfläche aus können Sie diese Themen aufrufen, indem Sie auf die Schaltfläche **Hilfe** des jeweiligen Dialogfelds klicken.

- "Hilfe zur Seite "Antivirus" des Dialogfelds "Updates downloaden"" auf Seite 776
- "Hilfe zu Antivirus-Tasks" auf Seite 779
- "Hilfe zu Antivirus-Einstellungen" auf Seite 781

Hilfe zur Seite "Antivirus" des Dialogfelds "Updates downloaden"

Informationen zur Seite "LANDesk Antivirus" im Dialogfeld "Updates downloaden"

Die Seite **LANDesk Antivirus** des Dialogfelds **Updates downloaden** verwenden Sie, um Einstellungen zum Download von Virendefinitionsdatei-Updates aus LANDesk Security Suite Diensten zu konfigurieren. Sie können Antivirusinhalt (Virendefinitionen/Musterdateien) herunterladen und angeben, welche Virendefinitionsdateien für die Verteilung an verwaltete Geräte verfügbar sind (sofort oder nach Ablauf eines Testzeitraums) und ob eine Sicherungskopie von Definitionsdateien angelegt werden soll.

Sie sollten beachten, dass die Definitionsliste auf der Seite **Updates** des Dialogfelds **Updates downloaden** mehrere Antivirus-Updates enthält, einschließlich eines Updates mit der Bezeichnung "LANDesk Antivirus-Updates". Wenn Sie diesen Typ auswählen, werden SOWOHL der vom Scanner erkannte Inhalt ALS AUCH die Updates für die Virendefinitionsdatei gedownloadet.

Antivirus-Updates sind Scannerdefinitionen, die Folgendes erkennen:

- Installation von gängigen Antivirus-Scanner-Engines (einschließlich des LANDesk Antivirus-Agenten)
- Scanstatus in Echtzeit (aktiviert oder deaktiviert)
- Scannerspezifische Musterdateiversionen (auf dem neuesten Stand oder veraltet)
- Datum des letzten Scans (ob der letzte Scan innerhalb des vom Administrator festgelegten maximal zulässigen Zeitraums erfolgte)

HINWEIS: Vom Antivirus-Scanner erkannter Inhalt im Vergleich zu Virendefinitionsinhalt
Antivirus-Updates erstrecken sich nicht auf die eigentlichen Virendefinitionsdateien (oder Musterdateien). Wenn Sie Antivirus-Updates eines anderen Herstellers herunterladen, wird nur von Scannern erkannter Inhalt in das Standardrepository heruntergeladen, scannerspezifische Virendefinitionsdateien werden dagegen nicht heruntergeladen. Wenn Sie jedoch LANDesk Antivirus-Updates herunterladen, werden SOWOHL vom Scanner erkannte Inhalte ALS AUCH die LANDesk Antivirus-spezifischen Virendefinitionsdateien heruntergeladen. LANDesk Antivirus-Virendefinitionsdateien werden in einen separaten Speicherort auf dem Coreserver gedownloadet. Das Standardrepository für Virendefinitionsdateien ist der Ordner \LDLogon\Antivirus\Bases.

Sie müssen über das erforderliche LANDesk Security Suite Inhaltsabonnement verfügen, um den jeweiligen Sicherheitsinhalt herunterladen zu können.

Eine Basisinstallation von LANDesk Management Suite ermöglicht es Ihnen, nach LANDesk Softwareupdates zu suchen und sie herunterzuladen sowie eigene benutzerdefinierte Definitionen zu erstellen und zu verwenden. Für alle anderen Arten von Sicherheitsinhalt, z. B. plattformspezifische Anfälligkeiten, Spyware und Virendefinitionsdateien (Musterdateien), benötigen Sie ein LANDesk Security Suite Inhaltsabonnement, das es Ihnen ermöglicht, die entsprechenden Definitionen herunterzuladen.

Informationen zu den Security Suite Inhaltsabonnements erhalten Sie von Ihrem Händler; oder besuchen Sie die LANDesk Website.

LANDesk Startseite

Führen Sie die folgenden Schritte aus, nachdem Sie die Inhalte, die Sie herunterladen möchten, angegeben und die gewünschten Optionen im Dialogfeld "Updates downloaden" festgelegt haben:

- Klicken Sie zum Ausführen eines sofortigen Downloads auf **Jetzt aktualisieren**. Falls Sie auf **Übernehmen** klicken, werden die angegebenen Einstellungen gespeichert und beim nächsten Öffnen dieses Dialogfelds angezeigt. Falls Sie auf **Schließen** klicken, werden Sie gefragt, ob Sie die Einstellungen speichern möchten.
- Klicken Sie zum Planen eines Tasks für das Herunterladen von Sicherheits- und Patchinhalten auf **Update planen**, um das Dialogfeld **Informationen zum geplanten Update** zu öffnen. Geben Sie einen Namen für den Task ein, überprüfen Sie die Informationen für den Task und klicken Sie dann auf **OK**, um den Task zu den geplanten Tasks hinzuzufügen.

WICHTIG: Taskspezifische Einstellungen und globale Einstellungen
Beachten Sie, dass nur die Definitionstyp-, Sprach- sowie Definitions- und Patch-Downloadeinstellungen gespeichert und mit einem spezifischen Task während dessen Erstellung verknüpft werden. Diese drei Einstellungen gelten als taskspezifisch. Alle anderen Einstellungen auf den anderen Seiten des Dialogfeldes **Updates downloaden** sind global, d. h., sie gelten für alle nachfolgenden Downloadtasks für Sicherheitsinhalte. Die globalen Einstellungen umfassen: Patchdownload-Speicherort, Proxyserver, Spyware-Autofix, Sicherheitsalarme und Antivirus. Jedes Mal, wenn Sie eine globale Einstellung ändern, gilt diese Änderung für alle Sicherheitsinhalt-Downloadtasks von diesem Punkt an.

Wenn Sie die Änderungen speichern möchten, die Sie auf einer beliebigen Seite dieses Dialogfelds vorgenommen haben, können Sie dies jederzeit durch Klicken auf **Übernehmen** tun.

Die Seite **LANDesk Antivirus** enthält die folgenden Optionen:

- **Virendefinitionen, deren Verteilung genehmigt wurde:** Zeigt das Datum und die Versionsnummer der zuletzt genehmigten Virendefinitionsdateien an, die jetzt für die Verteilung an Ihre verwalteten Geräte zur Verfügung stehen. Genehmigte Virendefinitionen befinden sich im Standardordner (\LDLogon\Antivirus\Bases), von dem aus sie auf Zielgeräten als Teil eines Scans auf Abruf und als Teil geplanter Antivirusscans bereitgestellt werden. Der genaue Zeitpunkt des Virendefinitionsdatei-Updates (das von dem LANDesk Security Suite Webservice heruntergeladen wurde, der über die neuesten bekannten Musterdateien verfügt,) wird in Klammern unterhalb dieses Felds angezeigt.
- **Virendefinitionen, die zurzeit einem Pilottest unterzogen werden:** Beachten Sie, dass diese Liste nur dann angezeigt wird, wenn Sie die Option **Zunächst auf einen Pilottest beschränken** ausgewählt haben. Zeigt das Datum und die Versionsnummer der Virendefinitionsdateien an, die sich derzeit im Pilotordner befinden, sofern Sie Virendefinitionen in diesen Speicherort gedownloadet haben. Mithilfe von Pilottests können Sie sich von der Gültigkeit und Nützlichkeit einer Virendefinition überzeugen, bevor sie von Ihnen zum Scannen Ihrer Geräte auf Viren eingesetzt wird. Virendefinitionen, die in den Pilottest-Ordner gedownloadet wurden, können auf entsprechend festgelegten "Test"-Zielgeräten bereitgestellt werden.

- **Virendefinitionsupdates – Wenn neue Virendefinitionsdateien von LANDesk gedownloadet werden:**
    - **Sofort genehmigen (auf allen Computern bereitstellen):** Lädt Virendefinitionen direkt in den Standardordner (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8). In den Standardordner heruntergeladene Virendefinitionen werden genehmigt und können für die Durchführung von Antivirusscans auf Zielgeräten bereitgestellt werden.
    - **Zunächst auf einen Pilottest beschränken:** Lädt Virendefinitionsdateien zu Testzwecken in den Pilotordner. Virendefinitionen im Pilotordner können auf festgelegten Testgeräten bereitgestellt werden, bevor Sie sie auf Ihren verwalteten Geräten bereitstellen.
        - **Neueste Definitionen abrufen:** Startet einen sofortigen Virendefinitionsdatei-Download. Das Dialogfeld **Definitionen werden aktualisiert** informiert über den Verlauf des Downloads.
        - **Jetzt genehmigen:** Mit dieser Option können Sie Virendefinitionsdateien aus dem Pilotordner in den Standard-Virendefinitionsordner verschieben. Auf diese Weise können Sie auf Zielgeräten für Antivirusscans bereitgestellt werden.
        - **Genehmigung planen:** Öffnet das Extra "Geplante Tasks" mit einem neuen Task. Dort können Sie die Zeitplanoptionen festlegen ("Jetzt starten" oder an einem bestimmten Tag zu einer bestimmten Zeit starten und auch "Wiederholtes Auftreten" definieren). Dieser geplante Task lädt automatisch Virendefinitionsdateien aus dem Pilotordner in den Standardordner für Virendefinitionsdateien herunter (\LANDesk\ManagementSuite\ldlogon\antivirus8\win\bases8). (**HINWEIS:** Diese Option ist nur verfügbar, wenn Sie Virendefinitionsdatei-Updates nur für einen Pilottest zur Verfügung stellen. Mit dieser Option lässt sich zudem das Genehmigungsverfahren für Definitionsdateien automatisieren. Wenn Sie diese Option nicht aktivieren, müssen die Virendefinitionsdateien im Pilotordner mit der Schaltfläche **Jetzt genehmigen** manuell genehmigt werden.)
- **Virendefinitions-Backups**
    - **Backups von früheren Virendefinitionsdateien anfertigen:** Speichert Downloads von früheren Virendefinitionsdateien. Dies kann nützlich sein, wenn Sie auf eine ältere Definitionsdatei zurückgreifen müssen, um infizierte Dateien zu scannen, zu cleanen oder eine Virendefinitionsdatei wiederherzustellen, mit der ein bestimmtes Problem beseitigt werden konnte. (Sicherungskopien der Virendefinitionsdateien werden in separaten Ordnern (nach dem Datum und der Uhrzeit ihrer Erstellung benannt) in folgendem Verzeichnis gespeichert: \LDLogon\Antivirus\Backups\)
    - **Anzahl der beizubehaltenden Backups:** Gibt die Anzahl der zu speichernden Virendefinitionsdatei-Downloads an.
    - **Verlauf:** Listet alle verfügbaren Virendefinitionsdatei-Backups auf.
    - **Wiederherstellen:** Verschiebt das ausgewählte Virendefinitionsdatei-Backup in den Virenschutz-Standardordner, damit die Verteilung an Zielgeräte erfolgen kann.
    - **Löschen:** Entfernt das ausgewählte Virendefinitionsdatei-Backup dauerhaft vom Coreserver.
- **Jetzt downloaden:** Downloadet die ausgewählten Sicherheitsinhalte sofort. Das Dialogfeld **Definitionen werden aktualisiert** zeigt den Verlauf und Status des Downloads an.

- **Download planen:** Öffnet das Dialogfeld **Informationen zum geplanten Download**. In dieses Dialogfeld können Sie einen eindeutigen Namen für den Downloadtask eingeben, die Downloadeinstellungen überprüfen und durch Klicken auf OK den Task im Extra "Geplante Tasks" speichern. (Beachten Sie, dass nur die Definitionstyp-, Sprach- sowie Definitions- und Patch-Downloadeinstellungen gespeichert und zugewiesen werden, wenn Sie einen bestimmten Task erstellen.) Downloadeinstellungen auf den anderen Seiten dieses Dialogfeldes, z. B. der Speicherort für den Patchdownload sowie Proxy- und Alarmeinstellungen, sind global, d. h., sie gelten für alle Sicherheitsinhalt-Downloadtasks. Sie können diese Einstellungen jedoch jederzeit ändern; sie gelten dann von diesem Zeitpunkt an für alle Sicherheitsinhalt-Downloadtasks.)
- **Protokoll anzeigen:** Gibt Ihnen die Möglichkeit, den Speicherort und die Detailebene einer Prototolldatei mit Informationen zum Download von Virendefinitionsdateien zu wählen.
- **Übernehmen:** Speichert Ihre ausgewählten Downloadeinstellungen, damit sie für das Dialogfeld **Updates downloaden** übernommen und beim nächsten Öffnen des Dialogfelds angezeigt werden.
- **Schließen:** Schließt das Dialogfeld, ohne die letzten Einstellungsänderungen zu speichern.

Eine Beschreibung der Optionen auf den anderen Registerkarten des Dialogfelds **Updates downloaden** finden Sie unter "Informationen zum Dialogfeld "Updates downloaden"" auf Seite 654.

Hilfe zu Antivirus-Tasks

Informationen zum Dialogfeld "LANDesk Antivirus-Task erstellen"

Dieses Dialogfeld verwenden Sie zur Erstellung eines Tasks, der die Virendefinitionsdateien aktualisiert oder Antivirusscans auf Zielgeräten (mit Antivirus-Einstellungen) konfiguriert oder beides. Die Antivirus-Einstellungen bestimmen das Scannerverhalten, welche Objekte gescannt werden sowie die Optionen, die Endbenutzern zur Verfügung stehen.

HINWEIS: On-demand Antivirusscans
Unter Verwendung des Kontextmenüs können Sie auch bei Bedarf ("on Demand") einen Antivirusscan auf einem Gerät ausführen.

Dieses Dialogfeld enthält folgende Optionen:

- **Taskname:** Kennzeichnet den Antivirus-Scantask mithilfe eines eindeutigen Namens.
- **Auszuführende Aktionen:** Gibt an, welche Aufgabe der Task erfüllen soll. Sie können nur eine Aktion oder aber beide Aktionen auswählen.
  - **Virenschutzdefinitionen aktualisieren:** Gibt an, dass der Task die Virendefinitionsdateien auf der Basis der Einstellungen auf der Seite "Antivirus" des Dialogfelds "Updates downloaden" aktualisieren wird.
  - **Antivirusscan starten:** Gibt an, dass der Task einen Antivirusscan auf den Zielgeräten ausführen wird.

- **Geplanten Task erstellen:** Fügt den Scantask zum Fenster "Geplante Tasks" hinzu. Dort können Sie die Zeitplan- und Wiederholungsoptionen für den Task definieren und Zielgeräte zuweisen.
  - **Alle LANDesk Antivirus-Computer automatisch als Ziel auswählen:** Fügt verwaltete Geräte, die mit dem LANDesk Antivirus-Agenten konfiguriert wurden, der Zielgeräteliste des Tasks hinzu.
  - **Jetzt starten:** Führt den Antivirusscan auf Geräten aus, die über den LANDesk Antivirus-Agenten verfügen, und fügt ihn dem Tool "Geplante Tasks" hinzu, sobald Sie auf **OK** klicken.
  - **Virendefinitionen (einschließlich Pilotdefinition) auf dem Core aktualisieren:** Aktualisiert automatisch Virenmusterdateien, bevor der Scan gestartet wird (einschließlich Virendefinitionsdateien, die sich gegenwärtig im Pilotordner befinden). (Hinweis: Die oben erwähnte Option "Virenschutzdefinitionen aktualisieren" muss ausgewählt werden, damit diese Option verwendet werden kann.
- **Richtlinie erstellen:** Fügt den Antivirus-Scantask als Richtlinie zum Fenster "Geplante Tasks" hinzu. Dort können Sie die Richtlinienoptionen konfigurieren.
- **LANDesk Antivirus-Einstellungen:** Gibt die für den Scantasks verwendete Antivirus-Einstellungen an. Mithilfe der Antivirus-Einstellungen können Sie die Anzeige des LANDesk Antivirus-Symbols in der Symbolleiste des Geräts ein-/ausschalten, die Verfügbarkeit von interaktiven Optionen für Endbenutzer steuern, die Einstellungen in Bezug auf die Aktivierung von E-Mail-Scans und Echtzeitschutz festlegen, die zu scannenden Dateitypen und auszuschließenden Dateien und Ordner auswählen, infizierte Dateien unter Quarantäne stellen, Backups veranlassen und die Durchführung geplanter Antivirusscans und Virendefinitionsdatei-Updates konfigurieren. Wählen Sie eine der Einstellungen aus der Dropdownliste aus. Klicken Sie auf **Bearbeiten**, um die Optionen für die ausgewählten Einstellungen zu ändern. Klicken Sie auf **Konfigurieren**, um neue Einstellungen zu erstellen.
- **Virendefinitionsdateien:** Zeigt Informationen zu den derzeit heruntergeladenen Definitionsdateien an. Klicken Sie auf **Updates downloaden**, um zur Seite "LANDesk Antivirus" des Dialogfelds "Updates downloaden" zu gelangen und den Download einer Virendefinitionsdatei zu konfigurieren und zu planen.

Informationen zum Dialogfeld "LANDesk Antivirus - Jetzt scannen"

Über dieses Dialogfeld können Sie einen sofortigen Antivirusscan auf einem oder mehreren Zielgeräten veranlassen.

1. Klicken Sie mit der rechten Maustaste auf das gewünschte Gerät (bzw. auf eine Mehrfachauswahl mit bis zu 20 Geräten) und klicken Sie dann auf **LANDesk Antivirus - Jetzt scannen**
2. Wählen Sie die Antivirus-Einstellungen aus.
3. Geben Sie an, ob die Virendefinitionsdateien vor dem Scannen aktualisiert werden sollen. (Hinweis: Die Option aktualisiert automatisch Virenmusterdateien, bevor der Scan gestartet wird, einschließlich Virendefinitionsdateien, die sich gegenwärtig im Pilotordner befinden.
4. Klicken Sie auf **OK**.

Hilfe zu Antivirus-Einstellungen

Informationen zum Dialogfeld "LANDesk Antivirus-Einstellungen"

Dieses Dialogfeld verwenden Sie zum Erstellen und Bearbeiten von Antivirus-Einstellungen. Mithilfe der Antivirus-Einstellungen können Sie die Anzeige des LANDesk Antivirus-Symbols in der Symbolleiste des Geräts ein-/ausschalten, die Verfügbarkeit von interaktiven Optionen für Endbenutzer steuern, die Einstellungen in Bezug auf die Aktivierung von E-Mail-Scans und Echtzeitschutz festlegen, die zu scannenden Dateitypen und auszuschließenden Dateien und Ordner auswählen, infizierte Dateien unter Quarantäne stellen, Backups veranlassen und die Durchführung geplanter Antivirusscans und Virendefinitionsdatei-Updates konfigurieren.

Wenn Sie die Standard-Virenschutzeinstellungen eines Geräts ändern möchten, ohne erneut einen Antivirus-Scantask bereitzustellen, sollten Sie die gewünschte Änderung an einer beliebigen Einstellung auf einer der zahlreichen Seiten des Dialogfelds "Antivirus-Einstellungen" vornehmen, die neuen Einstellungen einem Einstellungsänderungstask zuordnen und diesen Task dann auf Zielgeräten bereitstellen.

Nachdem Sie Antivirus-Einstellungen konfiguriert haben, können Sie sie auf Antivirus-Scantasks und auf Einstellungsänderungstasks anwenden.

Dieses Dialogfeld umfasst die folgende Seiten:

- "Informationen zur Seite "Antivirus: Allgemeine Einstellungen"" auf Seite 781
- "Informationen zur Seite "Antivirus: Echtzeitschutz"" auf Seite 782
- "Informationen zur Seite "Antivirus: Virenscan"" auf Seite 784
- "Informationen zur Seite "Antivirus: Geplanter Scan"" auf Seite 786
- "Informationen zur Seite "Antivirus: Virendefinitionsupdates"" auf Seite 788
- "Informationen zur Seite "Antivirus: Legacy-Virendefinitionsupdates"" auf Seite 789
- "Informationen zur Seite "Antivirus: Quarantäne/Sicherung"" auf Seite 790

Informationen zur Seite "Antivirus: Allgemeine Einstellungen"

Diese Seite verwenden Sie zum Konfigurieren der grundlegenden Antivirus-Scanner-Einstellungen auf Zielgeräten.

Diese Seite enthält folgende Optionen:

- **Name:** Kennzeichnet die Antivirus-Einstellungen mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Einstellungen" in einem Dialogfeld zu einem Antivirus-Scantask angezeigt.
- **LANDesk Antivirus-Taskleistensymbol anzeigen:** Zeigt das LANDesk Antivirus-Symbol auf der Taskleiste des Geräts an. Ob dieses Symbol angezeigt wird, hängt vom Virenschutzstatus ab (es wird angezeigt, wenn Echtzeitschutz aktiviert ist). Wenn ein gelbes Pfeilsymbol angezeigt wird, ist der Echtzeitschutz aktiviert (d. h., das Gerät wird fortlaufend auf Virenbefall überwacht). Wenn das Symbol grau dargestellt wird, ist der Echtzeitschutz nicht aktiviert.

  HINWEIS: Endbenutzer können auf das Symbol doppelklicken, um den LANDesk Antivirus-Client zu öffnen und Tasks auszuführen. Darüber hinaus können sie mit der rechten Maustaste auf das Symbol klicken, um das Kontextmenü zu öffnen und die Option zum Ausführen eines Scans und Aktualisieren von Virenschutzdateien auszuwählen.

- **E-Mail-Scan aktivieren:** Aktiviert E-Mail-Scans in Echtzeit auf Zielgeräten. E-Mail-Scans in Echtzeit ermöglichen eine fortlaufende Überwachung eingehender und ausgehender E-Mail-Nachrichten (unterstützte Anwendung: Microsoft Outlook), indem sowohl der Textkörpers der Nachricht als auch der Nachrichtenanhang auf Viren überprüft wird. Erkannte Viren werden entfernt.
- **Scannen zum Kontextmenü hinzufügen:** Stellt auf dem LANDesk Antivirus-Client eine Option zur Verfügung, mit der Endbenutzer eine Datei, eine Dateigruppe, einen Ordner oder eine Ordnergruppe auswählen und dann mit der rechten Maustaste klicken können, um einen Antivirusscan auszuführen.
- **Zusätzlich zum Virenscan nach riskanter Software suchen (erweiterte Datenbank):** Stellt auf dem LANDesk Antivirus-Client eine Option zur Verfügung, die es Endbenutzern ermöglicht, ihre Systeme mithilfe einer erweiterten Datenbank, die auf verwaltete Geräte geladen wird, auf Riskware (FTP, IRC, Remotesteuerungsprogramme etc.) zu scannen.
- **Zulassen, dass Benutzer Dateien und Ordner zur Liste "Vertrauenswürdige Elemente" hinzufügen:** Stellt auf dem LANDesk Antivirus-Client eine Option zur Verfügung, mit der Benutzer Dateien und Ordner angeben können, die nicht auf Viren gescannt werden sollen. In dieser Liste aufgeführte Dateien und Order werden vom Antivirusscan ignoriert. Benutzer sollten darauf hingewiesen werden, dass nur sichere Dateien in die Liste mit den vertrauenswürdigen Elementen verschoben werden dürfen.
- **CPU-Auslastung beim Scannen:** Hiermit lässt sich die CPU-Nutzung auf Zielcomputern steuern, wenn LANDesk Antivirus einen Antivirusscan ausführt.
- **Eigentümer:** Hiermit können Sie einen Eigentümer für die Antivirus-Einstellungen festlegen und auf diese Weise nicht genehmigte Änderungen verhindern. Nur der Eigentümer und Benutzer mit Administrator-Recht können auf die Einstellungen zugreifen und sie ändern. Andere Benutzer können die Einstellungen nur anzeigen. Die Option "Öffentlicher Benutzer" ermöglicht universellen Zugriff auf die Einstellungen.
- **Als Standard festlegen:** Legt die betreffenden Antivirus-Einstellungen (einschließlich der Optionseinstellungen auf allen Registerkarten des Dialogfelds "Antivirus-Einstellungen") als Standard auf Zielgeräten fest. Mit dieser Option legen Sie fest, dass während der Ausführung von Aktualisierungstasks für Scan- und Definitionsdateien die Standardeinstellungen zu verwenden sind, es sei denn, ein Antivirus-Scantask ist mit spezifischen Antivirus-Einstellungen verknüpft.
- **Standardeinstellungen wiederherstellen:** Stellt die vordefinierten Standardeinstellungen für alle Virenschutzoptionen auf den Registerkarten des Dialogfelds wieder her.

Informationen zur Seite "Antivirus: Echtzeitschutz"

Diese Seite verwenden Sie zum Aktivieren und Konfigurieren des Echtzeitdateischutzes, zum Festlegen, welche Dateien geschützt und ausgeschlossen werden sollen, und zum Konfigurieren der Endbenutzerbenachrichtigung.

Der Echtzeitschutz ist ein fortlaufender (im Hintergrund ausgeführter) Scan für spezielle Dateien, Ordner und Dateitypen (nach Erweiterung). Wenn der Echtzeitschutz aktiv ist, werden Dateien bei jedem Öffnen, Schließen, Kopieren oder Speichern auf Viren gescannt.

Wenn der Echtzeitschutz aktiviert ist, wird das LANDesk Antivirus-Taskleistensymbol in gelber Farbe dargestellt. Das Symbol ist grau, wenn der Echtzeitschutz ausgeschaltet ist.

Diese Seite enthält folgende Optionen:

- **Echtzeitdateischutz aktivieren:** Schaltet den Echtzeitdateischutz auf Zielgeräten ein. Der Echtzeitdateischutz läuft im Hintergrund ab und scannt in Übereinstimmung mit der heruntergeladenen Virendefinitionsdatei nach bekannten Viren.

- **Echtzeitmeldungen auf dem Client anzeigen:** Zeigt Nachrichten auf Zielgeräten an, um Benutzer über bestimmte LANDesk Antivirus-Aktivitäten zu informieren. Endbenutzer werden benachrichtigt, wenn eine infizierte Datei erkannt, unter Quarantäne gestellt, gelöscht, übersprungen oder von Viren befreit wird. In den Nachrichten-Dialogfenstern werden Pfad, Dateiname, der Name des Virus und eine Nachricht angezeigt, die den Benutzer anweist, sich an den Netzwerkadministrator zu wenden.
- **Zulassen, dass der Benutzer Echtzeitscans verzögern darf bis zu:** Stellt eine Option auf dem LANDesk Antivirus-Client bereit, mit der Endbenutzer den Echtzeitdateischutz für einen angegebenen Zeitraum ausschalten können. Sie sollten eine möglichst kurze Zeitspanne auswählen, damit der Echtzeitschutz nicht für einen längeren Zeitraum deaktiviert werden kann.
- **Netzwerkpfade ausschließen:** Beschränkt den Echzeitdateiscan auf lokale Laufwerke und schließt zugeordnete Netzwerklaufwerke aus.
- **Alle Dateitypen scannen:** Legt fest, dass alle Dateitypen auf dem Zielgerät von einem Antivirusscan gescannt werden. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Es empfiehlt sich deshalb, alle Dateitypen mit einem Scan auf Abruf anstatt Echtzeitschutz zu scannen.
- **Nur infizierbare Dateien scannen:** Gibt an, dass nur infizierbare Dateien vom Scan zu prüfen sind. Als infizierbar gelten alle Dateien, die als virenanfällig bekannt sind. Das Scannen auf infizierbare Dateien zu begrenzen ist effizienter, als alle Dateien zu scannen, da einige Viren nur bestimmte Dateitypen infizieren. Sie sollten es sich jedoch zur Angewohnheit machen, alle Dateien in regelmäßigen Abständen mit On-Demand-Scans zu überprüfen, um sicherzustellen, dass die Geräte virenfrei sind.

  HINWEIS: Infizierbare Dateitypen werden nicht anhand ihrer Dateierweiterung, sondern anhand ihrer Format-ID im Datei-Header identifiziert. Auf diese Weise wird sichergestellt, dass auch umbenannte Dateien gescannt werden. Zu den infizierbaren Dateien zählen folgende: Dokumentdateien wie Word- und Excel-Dateien, mit Dokumentdateien verbundene Vorlagendateien und Programmdateien wie Dynamic Link Libraries (.DLLs), Kommunikationsdateien (.COM), ausführbare Dateien (.EXEs) sowie andere Programmdateien. Weiter unten finden Sie eine umfassende Liste infizierbarer Dateitypen.

- **Zum Scannen nach möglichen Viren heuristische Methoden verwenden:** Nutzt beim Scannen von Zielgeräten die heuristische Analysekapazität des Scanners. Heuristische Scans versuchen, Dateien ausfindig zu machen, bei denen der Verdacht auf eine Vireninfektion besteht. Sie halten zu diesem Zweck gezielt nach verdächtigen Verhaltensweisen Ausschau, z. B. einem Programm, das sich selbst modifiziert, das sofort versucht, eine andere ausführbare Datei zu finden oder das nach dem Beenden modifiziert wird. (HINWEIS: Heuristische Scanverfahren können die Leistung auf verwalteten Geräten negativ beeinflussen.
- **Folgende Dateien und Ordner ausschließen:**
  - **Hinzufügen:** Öffnet das Dialogfeld **Ausgeschlossenen Pfad hinzufügen**. In diesem Dialogfeld können Sie neue Ausschlüsse erstellen, um die Dateien, Ordner oder Dateitypen (nach Erweiterung) anzugeben, die Sie von einem mit diesen Einstellungen verknüpften Antivirusscan ausschließen möchten.
  - **Bearbeiten:** Öffnet den ausgewählten Ausschluss, damit Sie Dateipfad, Dateinamen, Dateierweiterung und Variablen modifizieren können.
  - **Löschen:** Entfernt den ausgewählten Ausschluss aus den Antivirus-Einstellungen.

Informationen zum Dialogfeld "Ausgeschlossenen Pfad hinzufügen"

Dieses Dialogfeld (auf das Sie vom Dialogfeld "Echtzeitschutz" aus zugreifen) verwenden Sie, um Ausschlüsse hinzuzufügen, die für Objekte gelten, die weder von einem Antivirusscan noch vom Echtzeitschutz auf Viren gescannt werden. Antivirus-Scantasks (und Einstellungsänderungstasks), die mit dieser Antivirus-Einstellung verknüpft sind, verwenden diese Ausschlüsse.

Sie können bestimmte Dateien, ganze Ordner und Dateitypen anhand ihrer Erweiterung ausschließen.

Dieses Dialogfeld enthält folgende Optionen:

- **Typ:** Gibt an, welchen Objekttyp Sie vom Antivirusscan ausschließen möchten. Wählen Sie einen Typ aus und geben Sie dann die genauen Attribute in das Objektfeld ein.
- **Objekt:** Geben Sie den vollständigen Dateipfad und -namen der Datei oder des Ordners ein, den Sie ausschließen möchten (oder navigieren Sie zu dem entsprechenden Verzeichnis und wählen Sie die Datei bzw. den Ordner aus). Wenn Sie als Ausschlusskriterium die Dateierweiterung ausgewählt haben, geben Sie die Erweiterungszeichen in das Feld "Objekt" ein.
- **Variable einfügen:** Diese Option ermöglicht es Ihnen, Systemumgebungsvariablen zu verwenden, um den Pfad zu einem Ordner oder einem Objekt zu kennzeichnen, den/das Sie aus dem Antivirusscan oder Schutzbereich ausschließen möchten.

Informationen zur Seite "Antivirus: Virenscan"

Über die Optionen auf dieser Registerkarte geben Sie an, welche Dateien auf Viren gescannt und welche vom Scan ausgeschlossen werden sollen, und legen fest, ob mithilfe heuristischer Verfahren nach verdächtigen Dateien gesucht werden soll.

Diese Seite enthält folgende Optionen:

- **Alle Dateitypen scannen:** Legt fest, dass alle Dateitypen auf dem Zielgerät von einem Antivirusscan gescannt werden. Dieser Vorgang kann einige Zeit in Anspruch nehmen. Es empfiehlt sich deshalb, alle Dateitypen mit einem Scan auf Abruf anstatt Echtzeitschutz zu scannen.
- **Nur infizierbare Dateien scannen:** Gibt an, dass nur infizierbare Dateien vom Scan zu prüfen sind. Als infizierbar gelten alle Dateien, die als virenanfällig bekannt sind. Das Scannen auf infizierbare Dateien zu begrenzen ist effizienter, als alle Dateien zu scannen, da einige Viren nur bestimmte Dateitypen infizieren. Sie sollten es sich jedoch zur Angewohnheit machen, alle Dateien in regelmäßigen Abständen mit On-Demand-Scans zu überprüfen, um sicherzustellen, dass die Geräte virenfrei sind. Weiter unten finden Sie eine umfassende Liste infizierbarer Dateitypen.
- **Zum Scannen nach möglichen Viren heuristische Methoden verwenden:** Nutzt beim Scannen von Zielgeräten die heuristische Analysekapazität des Scanners. Heuristische Scans versuchen, Dateien ausfindig zu machen, bei denen der Verdacht besteht, mit einem Virus infiziert zu sein. Sie halten zu diesem Zweck gezielt nach verdächtigen Verhaltensweisen Ausschau, z. B. einem Programm, das sich selbst modifiziert, das sofort versucht, eine andere ausführbare Datei zu finden, oder das nach dem Beenden modifiziert wird. Heuristische Scanverfahren können die Leistung auf verwalteten Geräten negativ beeinflussen.

- **Folgende Dateien und Ordner ausschließen**
  - **Hinzufügen:** Öffnet das Dialogfeld **Ausgeschlossenen Pfad hinzufügen**. In diesem Dialogfeld können Sie neue Ausschlüsse erstellen, um die Dateien, Ordner oder Dateitypen (nach Erweiterung) anzugeben, die Sie von einem mit diesen Einstellungen verknüpften Antivirusscan ausschließen möchten.
  - **Bearbeiten:** Öffnet den ausgewählten Ausschluss, damit Sie Dateipfad, Dateinamen, Dateierweiterung und Variablen modifizieren können.
  - **Löschen:** Entfernt den ausgewählten Ausschluss aus den Antivirus-Einstellungen.
- **Registrierung bereinigen:** Legt fest, dass die Registry in den Antivirusscan einbezogen wird.

WICHTIG: System-Restore-Point scannen
LANDesk Antivirus scannt die Dateien in jedem System-Restore-Point-Ordner, der auf dem verwalteten Gerät vorhanden ist.

Infizierbare Dateitypen

Infizierbare Dateitypen werden nicht anhand ihrer Dateierweiterung, sondern anhand ihrer Format-ID im Datei-Header identifiziert. Auf diese Weise wird sichergestellt, dass auch umbenannte Dateien gescannt werden.

Zu den infizierbaren Dateien zählen folgende: Dokumentdateien wie Word- und Excel-Dateien, mit Dokumentdateien verbundene Vorlagendateien und Programmdateien wie Dynamic Link Libraries (.DLLs), Kommunikationsdateien (.COM), ausführbare Dateien (.EXEs) sowie andere Programmdateien. Nachstehend finden Sie eine nach der Standard- oder Original-Dateierweiterung des Dateiformats sortierte Liste infizierbarer Dateitypen.

- ACM
- ACV
- ADT
- AX
- BAT
- BIN
- BTM
- CLA
- COM
- CPL
- CSC
- CSH
- DLL
- DOC
- DOT
- DRV
- EXE
- HLP
- HTA
- HTM
- HTML

- HTT
- INF
- INI
- JS
- JSE
- JTD
- MDB
- MSO
- OBD
- OBT
- OCX
- PIF
- PL
- PM
- POT
- PPS
- PPT
- RTF
- SCR
- SH
- SHB
- SHS
- SMM
- SYS
- VBE
- VBS
- VSD
- VSS
- VST
- VXD
- WSF
- WSH

Informationen zur Seite "Antivirus: Geplanter Scan"

Diese Registerkarte verwenden Sie zum Aktivieren und Konfigurieren eines wiederkehrenden Antivirusscans auf Zielgeräten.

HINWEIS: LANDesk Antivirus-Scantypen
Sie können Ihre verwalteten Geräte mithilfe geplanter Scans, On-Demand-Scans und mit Datei- und E-Mail-Echtzeitschutz auf Viren prüfen lassen. Endbenutzer haben zudem die Möglichkeit, On-Demand-Scans ihres eigenen Computers auszuführen.

Diese Seite enthält folgende Optionen:

- **LANDesk Antivirus führt nach einem zeitlich festgelegten Plan einen Virenscan auf Geräten aus:** Aktiviert einen wiederkehrenden Antivirusscan, der auf Zielgeräten in Übereinstimmung mit der von Ihnen angegebenen Startzeit, Häufigkeit, Zeitbeschränkung und Bandbreitenanforderung ausgeführt wird.
- **Einstellungen ändern:** Öffnet das Dialogfeld "Planen". In diesem Dialogfeld können Sie die Zeitplanoptionen festlegen. Weitere Informationen erhalten Sie unter "Informationen zum Dialogfeld "Regelmäßige Virenschutzscans planen"" auf Seite 787.
- **Benutzer darf Scans planen:** Hiermit können Benutzer einen lokal geplanten Antivirusscan auf ihren eigenen Computern erstellen.

Informationen zum Dialogfeld "Regelmäßige Virenschutzscans planen"

Wenn Sie möchten, dass diese Antivirus-Einstellungen einen wiederkehrenden Antivirusscan einschließen, verwenden Sie dieses Dialogfeld, um Einstellungen für Startzeit, Häufigkeit, Uhrzeitbeschränkung und Bandbreitenanforderungen festzulegen. Mit diesen Einstellungen verknüpfte Antivirus-Scantasks (und Einstellungsänderungstasks) verwenden die hier definierten Regeln.

Alle Kriterien, die Sie in diesem Dialogfeld konfigurieren, müssen erfüllt sein, bevor der Task ausgeführt wird. Wenn Sie z. B. einen Zeitplan konfigurieren, der jeden Tag zwischen 8 und 9 Uhr wiederholt wird und dessen **Gerätezustand** "**Desktop muss gesperrt sein**" ist, dann wird der Task nur zwischen 8 und 9 Uhr ausgeführt, WENN das Gerät gesperrt ist.

Dieses Dialogfeld enthält folgende Optionen:

- **Start:** Klicken Sie auf diese Option, um einen Kalender anzuzeigen, in dem Sie den Tag angeben, an dem der Task starten soll. Wenn Sie einen Tag auswählen, können Sie auch die Tageszeit eingeben. Die Standardwerte für diese Optionen sind das aktuelle Datum und die aktuelle Uhrzeit.
- **Wiederholen nach:** Konfiguriert den Scan für die Ausführung in regelmäßigen Abständen. Wählen Sie die Anzahl der Minuten, Stunden und Tage aus, um festzulegen, wie oft der Task wiederholt wird.
- **Zeitbereich:** Wenn Sie möchten, dass der Task zwischen bestimmten Stunden ausgeführt wird, wählen Sie die Start- und Endzeit aus. Die Stunden werden im 24-Stunden-Zeitformat angegeben.
- **Wöchentlich zwischen:** Wenn Sie möchten, dass der Task zwischen bestimmten Wochentagen ausgeführt wird, wählen Sie den ersten und letzten Tag aus.
- **Monatlich zwischen:** Wenn Sie möchten, dass der Task zwischen bestimmten Tagen des Monats ausgeführt wird, wählen Sie das Anfangs- und Enddatum aus.

- **Min. Bandbreite:** Beim Konfigurieren von Local Scheduler-Befehlen können Sie angeben, welche Bandbreitenkriterien mindestens erfüllt sein müssen, damit der Task ausgeführt werden kann. Der Bandbreitentest besteht aus Netzwerkdaten, die an ein von Ihnen angegebenes Gerät übermittelt werden. Zu dem Zeitpunkt, zu dem der Task ausgeführt werden soll, sendet jedes Gerät, das den Local Scheduler-Task ausführt, eine kleine Menge ICMP-Netzwerkdaten an den von Ihnen angegebenen Gerät und wertet die Übertragungsleistung aus. Wenn das Zielgerät für den Test nicht verfügbar ist, wird der Task nicht ausgeführt. Sie können eine der folgende Optionen als Mindestbandbreite für Datenübertragungen wählen:
  - **RAS:** Der Task wird ausgeführt, wenn die Netzwerkverbindung des Geräts mit dem Zielgerät mindestens RAS- oder DFÜ-Geschwindigkeit erreicht (wie vom Netzwerk-API erkannt). Wenn Sie diese Option auswählen, bedeutet dies im Allgemeinen, dass der Task immer ausgeführt wird, wenn das Gerät über eine Netzwerkverbindung verfügt.
  - **WAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielgerät mindestens WAN-Geschwindigkeit erreicht. WAN-Geschwindigkeit wird als Nicht-RAS-Verbindung definiert, die langsamer als der LAN-Grenzwert ist.
  - **LAN:** Der Task wird ausgeführt, wenn die Verbindung des Geräts mit dem Zielgerät die LAN-Geschwindigkeitseinstellungen überschreitet. Als LAN-Geschwindigkeit wird standardmäßig jede Geschwindigkeit von mehr als 262.144 Bit/s definiert. Sie können den LAN-Grenzwert in der Agentenkonfiguration festlegen (Seite **Extras > Konfiguration > Agentenkonfiguration > Bandbreitenerkennung**). Die Änderungen werden erst wirksam, nachdem Sie die aktualisierte Konfiguration auf Geräten bereitgestellt haben.
  - **Computername:** Kennzeichnet den zum Testen der Gerätebandbreite verwendeten Computer. Die Testübertragung erfolgt zwischen einem Zielgerät und diesem Computer.
- **Gerätestatus:** Wenn die Ausführungskriterien für den Task einen Gerätestatus enthalten sollen, wählen Sie einen Status aus der Dropdownliste aus.
- **Nach Gesamtfilterablauf zusätzlich eine willkürliche Verzögerung einlegen:** Wenn Sie zusätzliche willkürliche Verzögerung wünschen, verwenden Sie diese Option. Wenn Sie eine zufällige Verzögerung auswählen, die Ihre für den Task konfigurierten Zeitbeschränkungen überschreitet, kann der Task nicht ausgeführt werden, wenn der Zufälligkeitswert für den Task außerhalb der konfigurierten Zeitbeschränkungen liegt.
  - **Verzögerung bis zu:** Wählen Sie die zusätzliche willkürliche Verzögerung aus, die zur Anwendung kommen soll.
  - **Und mindestens:** Wenn Sie möchten, dass der Task vor der Ausführung mindestens eine gewisse Zeit abwartet, wählen Sie diese Option. Wenn Sie beispielsweise einen Inventarscan planen, könnten Sie hier eine 5 eingeben, damit ein Computer Zeit zum Booten hat, bevor der Scan beginnt, wodurch die Reaktionsfähigkeit des PCs für den Benutzer verbessert wird.

Informationen zur Seite "Antivirus: Virendefinitionsupdates"

Diese Seite verwenden Sie zum Konfigurieren von Zeitplänen für Virendefinitions- bzw. Musterdateiupdates, Benutzerdownload- und Zugriffsoptionen für Geräte mit diesen Antivirus-Einstellungen.

Diese Seite enthält folgende Optionen:

- **Pilotversion von Virenschutz-Definitionsdateien downloaden:** Laden Sie Virendefinitionsdateien aus dem Pilottest-Ordner anstatt aus dem Standardpool (\LDLogon\Antivirus\Bases) des Coreservers. Virendefinitionen im Pilotordner können von einer speziell autorisierten Benutzergruppe zum Testen der Virendefinitionen vor ihrer Bereitstellung im gesamten Netzwerk gedownloadet werden. Wenn Sie einen Antivirus-Scantask erstellen, können Sie auch eine Option zum Downloaden der neuesten

Virendefinitionsupdates auswählen, einschließlich derjenigen, die sich im Pilottest-Ordner befinden. Anschließend können Sie eine Verknüpfung für Antivirus-Einstellungen konfigurieren (mit der Option "Pilotversion von Virenschutz-Definitionsdateien downloaden:" im aktivierten Zustand), um sicherzustellen, dass die Testgeräte die neuesten bekannten Virendefinitionsdateien erhalten. Wenn die Option "Pilotversion von Virenschutz-Definitionsdateien downloaden" ausgewählt ist, werden im Standardordner (\LDLogon\Antivirus\Bases) gespeicherte Virendefinitionsdateien nicht gedownloadet.

- **Benutzer dürfen Virendefinitionsupdates downloaden:** Gibt Endbenutzern an Zielgeräten die Möglichkeit, Virendefinitionsdateien auf eigene Initiative herunterzuladen. Diese Option wird auf dem LANDesk Antivirus-Client angezeigt und kann von diesem Dialogfeld und durch Klicken mit der rechten Maustaste auf das LANDesk Antivirus-Symbol in der Symbolleiste geöffnet werden.

  HINWEIS: Wenn ein Benutzer Virendefinitionsdateien downloadet, versucht das Gerät, in der folgenden Reihenfolge eine Verbindung mit Servern herzustellen: 1) Bevorzugter Server (falls ein Server konfiguriert wurde), 2) Coreserver und 3) LANDesk Security Suite Inhaltsserver (Internet).
- **Download von Virendefinitionsupdates:** Gibt die Quellwebsite an, von der die Virendefinitionsdateien gedownloadet werden. Je nachdem welche Option Sie hier in der Dropdownliste auswählen, wird eine oder beide der nachstehend beschriebenen Optionen für die Site der Downloadquelle (Coreserver und/oder Sicherheitsinhaltsserver im Internet) aktiviert und kann dann konfiguriert werden. (**HINWEIS:** Internet-Downloadoptionen werden auf der Seite **Legacy-Virendefinitionsupdates** konfiguriert.)
- **Core-Downloadoptionen:** Hier können Sie die Coreservereinstellungen konfigurieren, wenn Sie eine der beiden Optionen für die Site der Downloadquelle ausgewählt haben, die den Core einschließt.
  - **Peer-Download deaktivieren:** Verhindert den Download von Virendefinitionsdateien per Peer-Download (vom lokalen Cache oder einem Peer in derselben Multicast-Domäne).
  - **Bevorzugten Server deaktivieren:** Verhindert Downloads von Virendefinitionsdateien über einen bevorzugten Server. Weitere Information zu bevorzugten Servern finden Sie unter "Softwareverteilung/Verteilungspakete/Verteilungsmethoden" auf Seite 269.
- **Virendefinitionsupdates planen:** Aktiviert ein wiederkehrendes Virendefinitionsdatei-Update, das auf Zielgeräten in Übereinstimmung mit der von Ihnen angegebenen Startzeit, Häufigkeit, Zeitbeschränkung und Bandbreitenanforderung ausgeführt wird.
- **Zeitplan ändern:** Öffnet das Dialogfeld "Planen". In diesem Dialogfeld können Sie die Zeitplanoptionen angeben.

Informationen zum Dialogfeld "Regelmäßige Antivirus-Updates planen"

Wenn diese Antivirus-Einstellungen ein wiederkehrendes Virendefinitionsupdate einschließen sollen, können Sie mit diesem Dialogfeld Einstellungen für Startzeit, Häufigkeit, Uhrzeitbeschränkung und Bandbreitenanforderungen festlegen. Mit diesen Einstellungen verknüpfte Antivirus-Scantasks (und Einstellungsänderungstasks) verwenden die hier definierten Regeln.

Informationen zu den Optionen finden Sie oben unter "Informationen zum Dialogfeld "Regelmäßige Virenschutzscans planen"" auf Seite 787, da es sich um eine allgemeines Dialogfeld handelt.

Informationen zur Seite "Antivirus: Legacy-Virendefinitionsupdates"

Diese Seite verwenden Sie zum Konfigurieren der Einstellungen für Legacy-Virendefinitionsupdates sowie der Einstellungen für den LANDesk Security Suite Inhaltsserver, wenn Sie oben eine der Optionen für die Site der Downloadquelle ausgewählt haben, die das Internet einschließt.

Diese Seite enthält folgende Optionen:

- **Updates in einer Datei downloaden, wenn Anzahl der geänderten Dateien größer ist als:** Gibt die maximale Anzahl der neuen oder aktualisierten einzelnen Virusdefinitionsdateien an, die separat heruntergeladen werden, bevor der Download in einer einzigen komprimierte Datei erfolgt.
- **Internet-Downloadoptionen:** Hier können Sie die Einstellungen für den Sicherheitsinhaltsserver konfigurieren, wenn Sie eine der beiden Optionen für die Site der Downloadquelle ausgewählt haben, die das Internet einschließt.
    - **Quellsite:** Gibt den Sicherheitsinhaltsserver an, auf dem zum Download der neuesten Definitionen in Ihre Datenbank zugegriffen wird. Wählen Sie den Server aus, der Ihrem Standort am nächsten ist.
    - **Bei einem Ausfall auf alternative Quellsite zurückgreifen:** Unternimmt automatisch den Versuch, Updates von einem anderen Sicherheitsinhaltsserver herunterzuladen, der über die Virenschutzsignaturen verfügt, wenn die angegebene Quellsite keine Dateien übertragen kann.

WICHTIG: Legacy-Einstellungen gelten nur für ältere LANDesk Antivirus-Clients
Die auf dieser Seite angegebenen Einstellungen für Legacy-Virendefinitionsupdates gelten nur für ältere Versionen des LANDesk Antivirus-Clients, die auf Ihren verwalteten Geräten bereitgestellt wurden. Ältere Versionen des Clients werden typischerweise von einem LANDesk Coreserver der Version 8.8 SP3 oder älter installiert.

Informationen zur Seite "Antivirus: Quarantäne/Sicherung"

Diese Seite verwenden Sie, um die Größe des Quarantäne-/Sicherungsordners und die Objektwiederherstellungsoptionen zu konfigurieren, die Sie für die Endbenutzer bereitstellen möchten.

Diese Seite enthält folgende Optionen:

- **Größe des Quarantäne-/Sicherungsordners beschränken:** Hiermit können Sie die maximale Größe des freigegebenen Quarantäne-/Sicherungsordners auf Zielgeräten angeben. Dieser Ordner ist ein sicherer, isolierter Speicherbereich auf Geräten, auf denen LANDesk Antivirus installiert ist. Standardmäßig beträgt die Größe des Quarantänespeichers 50 MB; die unter Quarantäne gestellten Objekte werden standardmäßig 90 Tage gespeichert. Objekte im Quarantäne-/Sicherungsordner können erneut gescannt, gelöscht oder wiederhergestellt werden.

  HINWEIS: Objekte im Quarantäne-/Sicherungsordner werden automatisch mit den neuesten Virendefinitionen gescannt, sobald ein On-Demand-Scan ausgeführt oder die Antivirus-Musterdateien auf dem Gerät aktualisiert werden. Das System stellt auf diese Weise fest, ob infizierte Objekte vorhanden sind, die bereinigt werden können. Wenn der Virus aus einer Datei im dem Quarantäne-Ordner entfernt werden kann, wird diese automatisch wiederhergestellt und der Benutzer informiert.

  HINWEIS: Wird eine Vireninfektion entdeckt, wird die infizierte Datei zunächst (mit der Erweiterung *.bak im Ordner \LDClient\Antivirus\) gesichert und dann bereinigt. Wenn die Viren nicht entfernt werden können, wird die Originaldatei in den Quarantäneordner verschoben (mit der Erweiterung *.qar im Ordner \LDClient\Antivirus). Anschließend wird der Virenstring entfernt und die Datei verschlüsselt, damit sie weder geöffnet noch ausgeführt werden kann.

- **Maximale Größe:** Spezifiziert die maximale Größe des freigegebenen Quarantäne-/Sicherungsordners auf Geräten, die über den LANDesk Antivirus-Agenten verfügen.

- **Objekte werden wiederhergestellt:** Definiert die Rechte des Endbenutzers bezüglich der Wiederherstellung von Objekten, die unter Quarantäne gestellt wurden.
    - **Benutzer dürfen verdächtige Objekte wiederherstellen:** Gibt Endbenutzern die Möglichkeit, von einem Antivirusscan oder vom Echtzeitschutz identifizierte, verdächtige Objekte wiederherzustellen. Objekte gelten als verdächtig, wenn sie Code enthalten, der entweder manipuliert wurde oder dem Code eines bekannten Virus ähnelt. Verdächtige Objekte werden automatisch unter Quarantäne gestellt. Wenn diese Option ausgewählt wurde, können Endbenutzer die Originaldatei aus dem Quarantäneordner in einen angegebenen Zielordner oder in den Originalspeicherort verschieben, in dem die Datei vor dem Isolieren im Quarantäneordner, dem Entfernen der Viren oder dem Löschen gespeichert war. Hinweis: Wenn der Echtzeitschutz aktiv ist, wird die wiederhergestellte Datei gescannt und erneut unter Quarantäne gestellt, wenn sie nach wie vor Viren enthält.
    - **Benutzer dürfen infizierte Objekte und riskante Software wiederherstellen:** Gibt Endbenutzern die Möglichkeit, von einem Antivirusscan oder vom Echtzeitschutz identifizierte Objekte wiederherzustellen. Objekte gelten als infiziert, wenn sie destruktiven Code gemäß der Definition einer bekannten Virendefinitionsdatei (Muster oder Signatur) enthalten. Infizierte Objekte können außerdem verwalteten Geräten Schaden zufügen. Riskante Software ist im Wesentlichen Clientsoftware, die ein mögliches Risiko für den Endbenutzer darstellt. Zum Beispiel: FTP, IRC, MIrc, RAdmin oder Remotesteuerungs-Dienstprogrammsoftware. (Bei einem falsch-positiven Scanergebnis können Endbenutzer die Datei wiederherstellen, sofern sie sicher davon ausgehen können, dass die Datei sauber ist. Mit dieser Option können Benutzer Dateien in Netzwerkfreigaben wiederherstellen. Wenn Benutzer eine infizierte Datei im ursprünglichen Speicherort wiederherstellen, erkennt der nächste Antivirusscan denselben Virus, selbst wenn es sich um ein falsch-positives Resultat handelt, und fügt die Datei ganz einfach wieder in den Quarantänebereich ein.)
    - **Benutzer müssen zum Wiederherstellen von Objekten ein Kennwort eingeben:** Verlangt von Benutzern, die verdächtige oder infizierte Objekte bzw. riskante Software wiederherstellen möchten, die Eingabe des festgelegten Kennworts. Der Benutzer wird aufgefordert, das Kennwort einzugeben, sobald er versucht, das Objekt aus dem Quarantäne-/Sicherungsordner wiederherzustellen. Wenn Sie diese Option aktivieren, um unter Quarantäne gestellte Objekte mit einem Kennwort zu schützen, müssen Sie das Kennwort den Benutzern mitteilen, die Sie autorisieren möchten, diese Objekte wiederherzustellen.
    - **Kennwort:** Geben Sie das Kennwort ein, das die Benutzer zum Wiederherstellen von unter Quarantäne gestellten Objekten benötigen.
- **Löschen von Dateien:** Legt fest, ob Dateien automatisch gelöscht werden.
    - **Quarantänedateien automatisch löschen:** Gibt an, dass alle unter Quarantäne gestellte Dateien, die älter als der angegebene Zeitraum sind, automatisch gelöscht werden.
    - **Sicherungsdateien automatisch löschen:** Gibt an, dass alle Sicherungsdateien, die älter als der angegebene Zeitraum sind, automatisch gelöscht werden.

Hilfe zu LANDesk Antivirus Ultimate

Der Zugriff auf die Funktionen von LANDesk Antivirus Ultimate erfolgt über das Fenster des Extras "Agenteneinstellungen" (**Extras > Sicherheit > Agenteneinstellungen**).

Mit Antivirus können Sie Antivirusinhalt (d. h. Virendefinitionsdateien) herunterladen und verwalten, Antivirusscans konfigurieren und Anzeige-/Interaktionseinstellungen für den Antivirus-Scanner anpassen, mit denen festgelegt wird, wie der Scanner auf Zielgeräten angezeigt wird und arbeitet und welche interaktiven Optionen Endbenutzern zur Verfügung stehen. Außerdem können Sie auf den Virenschutz bezogene Informationen für gescannte Geräte anzeigen, Virenschutzalarmmeldungen aktivieren und Virenschutzberichte generieren.

Der Hauptabschnitt zu "LANDesk Antivirus" auf Seite 751 bietet eine Einführung zu diesem komplementären Sicherheitsverwaltungstool, das sowohl in LANDesk Management Suite als auch in LANDesk Security Suite enthalten ist. Im vorliegenden Abschnitt finden Sie einen Überblick, Informationen zum Abonnement von Antivirusinhalt sowie Schrittanleitungen zur Verwendung der Antivirusfunktionen.

Dieser Abschnitt enthält die nachstehend genannten Hilfethemen, in denen die Dialogfelder von Antivirus beschrieben werden. Von der Konsolenoberfläche aus können Sie diese Themen aufrufen, indem Sie auf die Schaltfläche **Hilfe** des jeweiligen Dialogfelds klicken.

Informationen zur Seite "LANDesk Antivirus Ultimate: Allgemein"

Diese Seite verwenden Sie zum Konfigurieren der grundlegenden LANDesk Antivirus-Scannereinstellungen auf Zielgeräten.

Diese Seite enthält folgende Optionen:

- **Name:** Kennzeichnet die Antivirus-Einstellungen mit einem eindeutigen Namen. Dieser Name wird in der Dropdownliste "Einstellungen" in einem Dialogfeld zu einem Antivirus-Scantask angezeigt.
- **Schutz:**
  - **Datei-Antivirus:** Aktiviert den Dateiscan in Echtzeit auf Zielgeräten.
  - **Mail-Antivirus:** Aktiviert E-Mail-Scans in Echtzeit auf Zielgeräten. E-Mail-Scans in Echtzeit ermöglichen eine fortlaufende Überwachung eingehender und ausgehender E-Mail-Nachrichten (unterstützte Anwendung: Microsoft Outlook), indem sowohl der Textkörper der Nachricht als auch der Nachrichtenanhang auf Viren überprüft wird. Erkannte Viren werden entfernt.
  - **Web-Antivirus:** Aktiviert den Echtzeitscan des Internetdatenverkehrs, von Website-URLs und Links auf Zielgeräten.
  - **IM-Antivirus:** Aktiviert den Echtzeitscan von Sofortnachrichten auf Zielgeräten.
  - **Schutz vor Netzwerkangriffen:** Aktiviert den Schutz vor Netzwerkangriffen, der angreifende Computer erkennt und für eine festgelegte Zeitspanne zur Liste der blockierten Geräte hinzufügt.
  - **Aktivitätsmonitor:** Aktiviert das Dienstprogramm Aktivitätsmonitor, das die Aktivitäten von Anwendungen auf Zielgeräten überwacht.
- **Berechtigungen:**
  - **Benutzer darf Schutzkomponenten deaktivieren für bis zu:** Gibt den Zeitraum an, während dem der Benutzer die oben aufgeführten Schutzkomponenten ausschalten darf.
  - **Benutzer darf Definitionen aktualisieren:** Lässt den Benutzer die Antivirus-Definitionsdateien bearbeiten.
  - **Benutzer darf Objekte wiederherstellen:** Lässt den Benutzer zu scannende Objekte wiederherstellen.
  - **Benutzer darf Einstellungen ändern:** Lässt den Benutzer Scans planen, Objekte aus Scans ausschließen und Web-URLs hinzufügen.

- **Benutzeroberfläche:**
  - **LANDesk Antivirus-Taskleistensymbol anzeigen:** Zeigt das LANDesk Antivirus-Symbol auf der Taskleiste des Geräts an. Ob dieses Symbol angezeigt wird, hängt vom Virenschutzstatus ab (es wird angezeigt, wenn Echtzeitschutz aktiviert ist). Wenn ein gelbes Pfeilsymbol angezeigt wird, ist der Echtzeitschutz aktiviert (d. h., das Gerät wird fortlaufend auf Virenbefall überwacht). Wenn das Symbol grau dargestellt wird, ist der Echtzeitschutz nicht aktiviert.
  - **Scannen zum Kontextmenü hinzufügen:**
- **Als Standard festlegen:** Legt die betreffenden Antivirus-Einstellungen (einschließlich der Optionseinstellungen auf allen Registerkarten des Dialogfelds "Antivirus-Einstellungen") als Standard auf Zielgeräten fest. Mit dieser Option legen Sie fest, dass während der Ausführung von Aktualisierungstasks für Scan- und Definitionsdateien die Standardeinstellungen zu verwenden sind, es sei denn, ein Antivirus-Scantask ist mit spezifischen Antivirus-Einstellungen verknüpft.

Informationen zur Seite "LANDesk Antivirus Ultimate: Schutz"

Auf dieser Seite konfigurieren Sie Schutzeinstellungen.

Diese Seite enthält folgende Optionen:

- **LANDesk Antivirus beim Systemstart starten:**
- **Technologie zur aktiven Desinfektion verwenden:**
- **Bedrohungen:**
  - **Malware:**
  - **Adware, Dialer, andere Programme:**
  - **Komprimierte Dateien:**
- **Ausschlüsse:**
  - **Echtzeit:**
  - **Virenscan:**
- **Hinzufügen:**
- **Bearbeiten:**
- **Löschen:**

Informationen zum Dialogfeld "Ausgeschlossenen Pfad hinzufügen"

Dieses Dialogfeld (auf das Sie vom Dialogfeld "Echtzeitschutz" aus zugreifen) verwenden Sie, um Ausschlüsse hinzuzufügen, die für Objekte gelten, die weder von einem Antivirusscan noch vom Echtzeitschutz auf Viren gescannt werden. Antivirus-Scantasks (und Einstellungsänderungstasks), die mit dieser Antivirus-Einstellung verknüpft sind, verwenden diese Ausschlüsse.

Sie können bestimmte Dateien, ganze Ordner und Dateitypen anhand ihrer Erweiterung ausschließen.

Dieses Dialogfeld enthält folgende Optionen:

- **Typ:** Gibt an, welchen Objekttyp Sie vom Antivirusscan ausschließen möchten. Wählen Sie einen Typ aus und geben Sie dann die genauen Attribute in das Objektfeld ein.
- **Objekt:** Geben Sie den vollständigen Dateipfad und -namen der Datei oder des Ordners ein, den Sie ausschließen möchten (oder navigieren Sie zu dem entsprechenden Verzeichnis und wählen Sie die Datei bzw. den Ordner aus). Wenn Sie als Ausschlusskriterium die Dateierweiterung ausgewählt haben, geben Sie die Erweiterungszeichen in das Feld "Objekt" ein.

- **Variable einfügen:** Diese Option ermöglicht es Ihnen, Systemumgebungsvariablen zu verwenden, um den Pfad zu einem Ordner oder einem Objekt zu kennzeichnen, den/das Sie aus dem Antivirusscan oder Schutzbereich ausschließen möchten.

Informationen zur Seite "LANDesk Antivirus Ultimate: Datei-Antivirus

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Datei-Antivirus aktivieren:**
- **Sicherheitsstufe:**
  - **Allgemein:** Dateitypen, Schutzbereich ...
  - **Leistung:** Heuristische Analyse, Nur neue und veränderte Dateien scannen, Archive scannen, Installation scannen, Eingebettete OLE-Objekte scannen, Erweitert ...
  - **Erweitert:** Scanmodus, Scantechnologien ...
- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Aktion wählen:**
  - **Desinfektion ausführen:**
  - **Löschen, wenn Desinfektion nicht möglich:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Mail-Antivirus

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Mail-Antivirus aktivieren:**
- **Sicherheitsstufe:**
  - **Allgemein:** Schutzbereich, Datenverkehr für POP3/SMTP/NNTP/IMAP, Erweitert: Microsoft Office Outlook-Plugin, Erweitert: The Bat!-Plugin, Angehängte Archive scannen ...
    - **Schutzbereich:** Eingehende und ausgehende Nachrichten, Nur eingehende Nachrichten ....
    - **Datenverkehr für POP3/SMTP/NNTP/IMAP:**
    - **Erweitert: Microsoft Office Outlook-Plugin:**
    - **Erweitert: The Bat!-Plugin:**
    - **Angehängte Archive scannen:** Archive nicht scannen, wenn größer als (MB), Archive nicht länger scannen als (s)
  - **Erweitert:** Heuristische Analyse (oberflächlicher Scan, mitteltiefer Scan, tiefgehender Scan)
- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Aktion wählen:** Desinfektion ausführen, Löschen, wenn Desinfektion nicht möglich ...

Informationen zur Seite "LANDesk Antivirus Ultimate: Web-Antivirus

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Web-Antivirus aktivieren:**
- **Sicherheitsstufe:**
- **Scanmethoden und Optimierung:**
  - **Links anhand der Datenbank für verdächtige Webadressen überprüfen:**
  - **Links anhand der Datenbank für Phishing-Webadressen überprüfen:**
  - **Heuristische Analyse zur Virenerkennung verwenden:**
  - **Heuristische Analyse zum Erkennen von Phishing-Links verwenden:**
  - **Zwischenspeicherung für Web-Datenverkehr limitieren**
- **Vertrauenswürdige Webadressen:**
  - **Web-Datenverkehr von vertrauenswürdigen Webadressen nicht scannen:**
  - **Hinzufügen:**
  - **Bearbeiten:**
  - **Löschen:**
- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Download blockieren:**
  - **Download zulassen:**

Informationen zur Seite "LANDesk Antivirus Ultimate: IM-Antivirus

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **IM-Antivirus aktivieren:**
- **Schutzbereich:**
  - **Eingehende und ausgehende Nachrichten:**
  - **Nur eingehende Nachrichten:**
- **Scanmethoden:**
  - **Links anhand der Datenbank für verdächtige Webadressen überprüfen:**
  - **Links anhand der Datenbank für Phishing-Webadressen überprüfen:**
  - **Heuristische Analyse:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Schutz vor Netzwerkangriffen

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Schutz vor Netzwerkangriffen aktivieren:**
- **Angreifenden Computer zur Sperrliste hinzufügen für (Minuten):**

Informationen zur Seite "LANDesk Antivirus Ultimate: Aktivitätsmonitor

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Aktivitätsmonitor aktivieren:**
- **Aktivitätsverlauf für Programme mit einer digitalen Signatur protokollieren**
- **Aktivität von Programmen mit digitaler Signatur nicht überwachen**
- **Rollback von Malware-Aktionen:**
- **Proaktiver Schutz:**
    - **Aktualisierbare Muster gefährlicher Aktivität verwenden (BSS):**
    - **Bei Erkennung von Malware-Aktivität:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Geplante Tasks"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Geplante Tasks:**
    - **Aktualisieren:**
    - **Vollständiger Scan:**
    - **Scan von wichtigen Bereichen:**
- **Hintergrundscantasks:**
    - **Scan bei Computerleerlauf ausführen:**
- **Wechseldatenträger beim Anschließen scannen:**
    - **Aktion beim Anschließen eines Wechseldatenträgers:**
    - **Maximale Größe des Wechseldatenträgers (MB):**

Informationen zur Seite "LANDesk Antivirus Ultimate: Aktualisieren"

Diese Seite verwenden Sie zum Konfigurieren von Zeitplänen für Virendefinitions- bzw. Musterdateiupdates, Benutzerdownload- und Zugriffsoptionen für Geräte mit diesen Antivirus-Einstellungen.

Diese Seite enthält folgende Optionen:

- **Pilotversion von Virenschutz-Definitionsdateien downloaden:** Laden Sie Virendefinitionsdateien aus dem Pilottest-Ordner anstatt aus dem Standardpool (\LDLogon\Antivirus\Bases) des Coreservers. Virendefinitionen im Pilotordner können von einer speziell autorisierten Benutzergruppe zum Testen der Virendefinitionen vor ihrer Bereitstellung im gesamten Netzwerk gedownloadet werden. Wenn Sie einen Antivirus-Scantask erstellen, können Sie auch eine Option zum Downloaden der neuesten Virendefinitionsupdates auswählen, einschließlich derjenigen, die sich im Pilottest-Ordner befinden. Anschließend können Sie eine Verknüpfung für Antivirus-Einstellungen konfigurieren (mit der Option "Pilotversion von Virenschutz-Definitionsdateien downloaden:" im aktivierten Zustand), um sicherzustellen, dass die Testgeräte die neuesten bekannten Virendefinitionsdateien erhalten. Wenn die Option "Pilotversion von Virenschutz-Definitionsdateien downloaden" ausgewählt ist, werden im Standardordner (\LDLogon\Antivirus\Bases) gespeicherte Virendefinitionsdateien nicht gedownloadet.

- **Benutzer dürfen Virendefinitionsupdates downloaden:** Gibt Endbenutzern an Zielgeräten die Möglichkeit, Virendefinitionsdateien auf eigene Initiative herunterzuladen. Diese Option wird auf dem LANDesk Antivirus-Client angezeigt und kann von diesem Dialogfeld und durch Klicken mit der rechten Maustaste auf das LANDesk Antivirus-Symbol in der Symbolleiste geöffnet werden.

  HINWEIS: Wenn ein Benutzer Virendefinitionsdateien downloadet, versucht das Gerät, in der folgenden Reihenfolge eine Verbindung mit Servern herzustellen: 1) Bevorzugter Server (falls ein Server konfiguriert wurde), 2) Coreserver und 3) LANDesk Security Suite Inhaltsserver (Internet).
- **Download von Virendefinitionsupdates:** Gibt die Quellwebsite an, von der die Virendefinitionsdateien gedownloadet werden. Je nachdem welche Option Sie hier in der Dropdownliste auswählen, wird eine oder beide der nachstehend beschriebenen Optionen für die Site der Downloadquelle (Coreserver und/oder Sicherheitsinhaltsserver im Internet) aktiviert und kann dann konfiguriert werden. (**HINWEIS:** Internet-Downloadoptionen werden auf der Seite **Legacy-Virendefinitionsupdates** konfiguriert.)
- **Core-Downloadoptionen:** Hier können Sie die Coreservereinstellungen konfigurieren, wenn Sie eine der beiden Optionen für die Site der Downloadquelle ausgewählt haben, die den Core einschließt.
  - **Peer-Download deaktivieren:** Verhindert den Download von Virendefinitionsdateien per Peer-Download (vom lokalen Cache oder einem Peer in derselben Multicast-Domäne).
  - **Bevorzugten Server deaktivieren:** Verhindert Downloads von Virendefinitionsdateien über einen bevorzugten Server. Weitere Information zu bevorzugten Servern finden Sie unter "Softwareverteilung/Verteilungspakete/Verteilungsmethoden" auf Seite 269.
- **Virendefinitionsupdates planen:** Aktiviert ein wiederkehrendes Virendefinitionsdatei-Update, das auf Zielgeräten in Übereinstimmung mit der von Ihnen angegebenen Startzeit, Häufigkeit, Zeitbeschränkung und Bandbreitenanforderung ausgeführt wird.
- **Zeitplan ändern:** Öffnet das Dialogfeld "Planen". In diesem Dialogfeld können Sie die Zeitplanoptionen angeben.

Informationen zur Seite "LANDesk Antivirus Ultimate: Vollständiger Scan"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Sicherheitsstufe:**
  - **Hoch:**
  - **Empfohlen:**
  - **Niedrig:**
- **Bereich:**
  - **Dateitypen:**
  - **Optimierung des Scanvorgangs:**
  - **Scan von zusammengesetzten Dateien:**
  - **Erweitert:**
- **Erweitert:**
  - **Scanmethoden:**
  - **Scantechnologien:** iSwift- oder iChecker-Technologie ...

- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Aktion ausführen:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Scan von wichtigen Bereichen"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Sicherheitsstufe:**
  - **Hoch:**
  - **Empfohlen:**
  - **Niedrig:**
- **Bereich:**
  - **Dateitypen:**
  - **Optimierung des Scanvorgangs:**
  - **Scan von zusammengesetzten Dateien:**
  - **Erweitert:**
- **Erweitert:**
  - **Scanmethoden:**
  - **Scantechnologien:** iSwift- oder iChecker-Technologie ...
- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Aktion ausführen:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Benutzerdefinierter Scan"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Sicherheitsstufe:**
  - **Hoch:**
  - **Empfohlen:**
  - **Niedrig:**
- **Bereich:**
  - **Dateitypen:**
  - **Optimierung des Scanvorgangs:**
  - **Scan von zusammengesetzten Dateien:**
  - **Erweitert:**
- **Erweitert:**
  - **Scanmethoden:**
  - **Scantechnologien:** iSwift- oder iChecker-Technologie ...

- **Aktion:**
  - **Aktion automatisch wählen:**
  - **Aktion ausführen:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Erweiterte Einstellungen"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Selbstschutz aktivieren:**
- **Externe Steuerung des Systemdienstes deaktivieren:**
- **Ressourcen für andere Programme freigeben:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Berichte und Speicher"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Berichtsparameter:**
- **Berichte speichern für maximal ... Tage:**
- **Maximale Dateigröße:**
- **Einstellungen für lokale Quarantäne und Backup:**
  - **Quarantänedateien nach jedem Update neu scannen:**
  - **Objekte speichern für maximal:**
  - **Maximale Speichergröße:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Benutzeroberfläche"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **"Protected by Kaspersky Lab" im Microsoft Windows-Anmeldebildschirm anzeigen:**
- **Animation des Symbols bei Taskausführung verwenden:**

Informationen zur Seite "LANDesk Antivirus Ultimate: Einstellungen importieren"

Sie verwenden diese Seite für die Konfiguration von ...

Diese Seite enthält folgende Optionen:

- **Einstellungen von einem Kaspersky Antivirus-Client importieren:**
  - **Aktuelle Konfiguration importiert von:**
  - **Kennwort nach dem Import löschen:**
  - **Datum:**
  - **Notizen:**

Verwandte Themen

LANDesk Antivirus-Wartungscenter / Hilfe zur Lizenzierung

Dieses Dialogfeld verwenden Sie, um die wesentlichen LANDesk Antivirus-Funktionen in Ihrer LANDesk Netzwerkumgebung zu konfigurieren.

WICHTIG: Ein gültiger LANDesk Antivirus-Lizenzschlüssel ist erforderlich
Damit Sie das Extra "LANDesk Antivirus" auf Ihrem Coreserver aktivieren und das Produkt zur Konfiguration und zum Schutz von Geräten verwenden können, ist ein gültiger Lizenzschlüssel erforderlich.

Sie können den Zeitrahmen für den Ablauf des LANDesk Antivirus Produktlizenzschlüssels festlegen und Zielgeräte auf Compliance scannen, einen neuen Lizenzschlüssel importieren, den Status der aktuellen Antivirus-Definitions- bzw. -Musterdateien auf Ihrem Server kontrollieren und die neusten Antivirus-Definitionsdateien herunterladen.

Informationen zum Dialogfeld "LANDesk Antivirus-Wartungscenter"

Dieses Dialogfeld enthält folgende Optionen:

- **Entfernen von anderer Antivirussoftware bestätigen:** Gibt an, dass Sie damit einverstanden sind, dass beim Installationsvorgang für LANDesk Antivirus alle anderen erkannten Antivirus-Softwareinstallationen von den Zielgeräten entfernt werden.
- **Ein LANDesk Antivirus-Lizenzschlüssel ist erforderlich:** Sie benötigen eine gültigen LANDesk Antivirus-Lizenz, um das LANDesk Antivirus-Produkte in Ihrer Netzwerkumgebung in vollem Umfang nutzen zu können.
    - **Neue Lizenz importieren:** Ermöglicht den Import eines gültigen LANDesk Antivirus-Lizenzschlüssels zur Aktivierung des Produkts auf Ihrem Coreserver.
- **Prüfen, ob es Clients gibt, bei denen die Lizenz demnächst abläuft:** Sie können die mit LANDesk Antivirus konfigurierten, verwalteten Geräten in Ihrem Netzwerk scannen, um herauszufinden, ob bei diesen das Ablaufdatum des Lizenzschlüssel demnächst erreicht ist.
    - **Ändern:** Hier können Sie die Anzahl der Tage angegeben, nach denen Ihr LANDesk Antivirus-Lizenzschlüssel ungültig wird.
    - **Neue Lizenz importieren:** Ermöglicht den Import eines gültigen LANDesk Antivirus-Lizenzschlüssels zur Aktivierung des Produkts auf Ihrem Coreserver.
    - **Clients anzeigen**: Hiermit können Sie anzeigen, welche verwalteten Geräte innerhalb der festgelegten Grenzwerte für den Ablauf des LANDesk Antivirus-Lizenzschlüssels liegen.
- **Die Virenschutzdefinitionen sind nicht auf dem neuesten Stand:** Zeigt an, dass die Antivirus-Definitionen (Muster- oder Signaturdateien) auf Ihrem Coreserver gemäß dem von Ihnen festgelegten Zeitrahmen nicht auf dem neusten Stand sind.
    - **Ändern:** Hier können Sie die Anzahl der Tage angeben, für deren Dauer die derzeit auf Ihrem Coreserver vorhandenen Antivirus-Definitionsdateien (Musterdateien) als aktuell gelten.
    - **Zu "Updates downloaden..." wechseln:** Öffnet das Dialogfeld **Updates downloaden** des Extras "Patch und Compliance". Dort können Sie die Einstellungen für den Download konfigurieren und einen Task zum Download von Antivirus-Definitionsdateien ausführen bzw. planen.

- **Dieses Dialogfeld automatisch anzeigen, wenn Antivirusaktionen erforderlich sind:** Sorgt dafür, dass das Dialogfeld **LANDesk Antivirus-Wartungscenter** in der LANDesk Konsole angezeigt wird, wenn einer oder mehrere der für die Optionen angegebenen Parameter erfüllt sind, und erinnert auf diese Weise daran, dass eine Aktion erforderlich ist.

Informationen zum Dialogfeld "LANDesk Antivirus – Lizenzinformationen"

Dieses Dialogfeld verwenden Sie, um Ihre aktuellen LANDesk Antivirus-Lizenzinformationen anzuzeigen und um einen neuen Lizenzschlüssel zu importieren.

WICHTIG: Nur LANDesk Administratoren
NUR Benutzer mit den Rechten eines LANDesk Administrators können einen LANDesk Antivirus-Lizenzschlüssel importieren.

Dieses Dialogfeld enthält folgende Optionen:

- **Neue Lizenzdatei importieren:**
  - **Pfad:** Navigieren Sie zu dem LANDesk Antivirus-Lizenzschlüssel, den Sie von LANDesk erhalten haben,
  - **Erstellungsdatum:** Zeigt das Erstellungsdatum des Lizenzschlüssels.
  - **Lizenznummer:** Zeigt die Lizenzschlüsselnummer.
  - **Lizenzinformationsnummer:** Zeigt die Lizenzinformationsnummer.
- **Aktuelle Lizenzinformationen:**
  - **Pfad:** Zeigt den Dateipfad zum LANDesk Antivirus-Lizenzschlüssel.
  - **Erstellungsdatum:** Zeigt das Erstellungsdatum des Lizenzschlüssels.
  - **Lizenznummer:** Zeigt die Lizenzschlüsselnummer.
  - **Lizenzinformationsnummer:** Zeigt die Lizenzinformationsnummer.
- **Bereitstellungsinformationen:**
  - **Aktivierte Knoten:** Zeigt die Anzahl der verwalteten Geräte an, die für LANDesk Antivirusschutz konfiguriert wurden und einen gültigen Lizenzschlüssel zur Ausführung haben.
  - **Maximale Anzahl:** Zeigt die maximale Anzahl von verwalteten Geräten an, die laut der Lizenz, die Sie von LANDesk erhalten und zur Aktivierung des Produkts "LANDesk Antivirus" auf Ihrem Coreserver verwendet haben, für LANDesk Antivirusschutz konfiguriert werden können.
  - **Frühestes Ablaufdatum:** Zeigt das Datum an, zu dem der nächste LANDesk Antivirus-Lizenzschlüssel mit Ablaufdatum tatsächlich ungültig wird.

Credant Data Protection

LANDesk Datenschutz – Übersicht

Das Extra LANDesk® Datenschutz mit Credant ist eine integrierte Partnerlösung, die Ihnen die Sammlung, Verfolgung und Anzeige von Informationen zum Status der Datenintegrität Ihrer verwalteten Geräte über die LANDesk Konsole ermöglicht.

Das Extra "LANDesk Datenschutz" nutzt zwei Partner-Tools von Credant: Credant Enterprise-Server (vorinstalliert und konfiguriert) und die Credant Agentensoftware, die auf Ihren mit LANDesk verwalteten Geräten bereitgestellt und ausgeführt wird.

Geschützt durch Datenschutzdienste

Wenn die Credant (Datenschutz)-Agentensoftware auf einem verwalteten Gerät installiert ist, gilt dieses Gerät als "geschützt" durch die integrierten Credant Datenschutzdienste. Zum Schutz der Daten auf geschützten (d. h. mit dem Datenschutzagenten konfigurierten) Geräten verwenden Credant Server eine richtlinienbasierte Datenverschlüsselung. LANDesk sammelt einfach diese Daten und meldet sie der Coredatenbank. Dort können LANDesk Administratoren die Datenschutzinformationen zu Geräten in der Inventaransicht der Konsole und in einem vordefinierten Bericht einsehen.

Die intelligente Datenverschlüsselung zeichnet sich durch folgende Merkmale und Funktionen aus:

- Unterstützung von standardkonformen Algorithmen (beispielsweise die nach FIPS 140-2 validierte 128-Bit-AES- und 256-Bit-AES-Verschlüsselung)
- Ergänzung des Microsoft Windows BitLocker
- Automatische Hinterlegung des Verschlüsselungsschlüssels für eine einfache sofortige Datenwiederherstellung
- Verschlüsselung der lokalen Security Account Manager (SAM)-Datenbank und Hash-Verschlüsselung des Domänenkennworts

Der LANDesk Coreserver sammelt Informationen aus der Credant (Datenschutz)-Serverdatenbank gemäß den Vorgaben des Datenschutzagenten, der auf dem jeweiligen verwalteten Gerät installiert ist.

WICHTIG: Credant Enterprise-Server müssen bereits in Ihrem Netzwerk installiert und eingerichtet worden sein
Damit Sie die neuen integrierten Extras und Funktionen für den Datenschutz in Verbindung mit Ihrer LANDesk Konsole nutzen können, müssen in Ihrer LANDesk Netzwerkumgebung bereits ein oder mehrere Credant Enterprise (Datenschutz)-Server installiert sein. Das heißt, sämtliche Installations- und Setuptasks für den Credant Server müssen VOR der Konfiguration (d. h. dem Hinzufügen) von Servern in der LANDesk Konsole und der Erstellung der Datenschutzverbindung zur LANDesk Coredatenbank durchgeführt worden sein. Zur Credant Website: Credant Enterprise Edition – Startseite.

Merkmale und Vorteile

LANDesk Datenschutz bietet Ihnen folgende Möglichkeiten:

- Konfigurieren einer Verbindung zwischen Ihrem LANDesk Coreserver und den Credant Servern, die für die Synchronisierung von Daten zwischen den betreffenden Datenbanken und den konfigurierten geschützten Geräten in Ihrem Netzwerk genutzt wird

- Anzeige von Informationen zum Datenschutz sowohl in der LANDesk Inventaransicht (unterhalb des Knotens **Data Protect**) als auch in der Übersichtsansicht, die per Rechtsklick zur Ansicht aufgerufen werden kann und unmittelbar Echtzeit-Scanergebnisse und -daten bereitstellt
- Start der nativen Credant Webkonsole
- Erstellung von Abfragen mit den in Credant (Datenschutz)-Datenbanken gesammelten Datenschutzinformationen, die nach bestimmten Attributen suchen, so wie dies auch bei anderen Arten von Inventardaten möglich ist. Diese Daten können auch in Standardspaltensätzen verwendet werden.
- Erstellung von geplanten Tasks für die automatische Sammlung von Informationen aus ALLEN Ihren Credant (Datenschutz)-Datenbanken
- Generierung eines Berichts zum Datenschutz, der Informationen zu allen Ihren geschützten Geräten in einem einzigen grafischen Bericht zusammenstellt

HINWEIS: LANDesk Datenschutz unterstützt mehrere Server und Datenbanken
Administratoren können Dateninformationen zu verwalteten Geräten von mehreren Datenschutz-Servern und -Datenbanken zusammentragen.

Wesentliche Datenschutztasks im Überblick

Die nachstehende Liste gibt einen Überblick über die wesentlichen Tasks zur Konfiguration, Implementierung und Verwendung der Datenschutzfunktionen. Die funktionsspezifischen Hilfethemen liefern detaillierte Informationen zu den Konzepten, Verfahren und Prozessen.

- Konfigurieren des Credant Enterprise-Servers bzw. der Credant Enterprise-Server
- Hinzufügen des Credant (Datenschutz)-Servers zu Ihrem LANDesk Management Suite Netzwerk über die Konsole
- Erstellen einer Datenbankverbindung zwischen dem Credant (Datenschutz)-Server und Ihrem LANDesk Coreserver
- Installieren der Credant Agentensoftware auf den von Ihnen verwalteten Geräten
- Anzeigen der Datenschutzinformationen in der Inventaransicht
- Anzeigen der Datenschutzinformationen in der Echtzeitübersicht
- Generieren von Berichten zum Datenschutz

WICHTIG: Der Credant Dienst darf auf den verwalteten Geräten KEINESFALLS gestoppt werden
Der Inventarscanner wurde beim LANDesk Datenschutz dahingehend verbessert, dass er erkennt, ob der Credant Agent auf dem verwalteten Gerät installiert ist, welche Versionsnummern vorliegen und ob die Dienste ausgeführt werden. Stoppen Sie den Credant Dienst KEINESFALLS, denn dadurch wird zwingend ein Neustart Ihres Computer ausgelöst.

Info zur Datenschutzoberfläche auf dem Endbenutzergerät

Für den Endbenutzer präsentiert sich die Software für den Datenschutzclient unter dem folgenden Produktnamen:

Credant Mobile Guardian Shield

Info zur Sicherheitsscan-Protokolldatei

Die Protokolldatei kann Systemadministratoren bei der Behebung bestimmter Probleme helfen.

Zusätzliche Informationsquellen

Navigieren Sie im LANDesk Help Center in den Hilfethemen zu LANDesk Management Suite oder führen Sie eine Suche mit einem bestimmten Schlüsselwort oder Ausdruck durch, um die von Ihnen gewünschten Informationen zu finden.

Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie hier:

LANDesk Benutzercommunity – Startseite

Verwandte Themen

"Datenschutz – Voraussetzungen" auf Seite 804

"Verwenden des Extras "Datenschutz"" auf Seite 805

"Info zum Datenschutzserver Seite "Servereigenschaften"" auf Seite 810

"Info zum Datenschutzserver: Seite "Datenbankverbindung"" auf Seite 811

"Anzeigen von Datenschutzinformationen im Inventar" auf Seite 806

"Generieren des Berichts zum Datenschutz" auf Seite 808

Datenschutz – Voraussetzungen

Bevor Sie Credant Server über die LANDesk Konsole konfigurieren (d. h. hinzufügen), stellen Sie sicher, dass folgende Systemvoraussetzungen erfüllt sind.

WICHTIG: Setup für Credant Enterprise-Server
LANDesk geht davon aus, dass Sie mit den Setupverfahren für den Credant Enterprise-Server vertraut sind und diesen vorab erforderlichen Task bereits ausgeführt haben. Nähere Informationen finden Sie auf der Website von Credant: Credant Enterprise Edition – Startseite.

Voraussetzungen

Vergewissern Sie sich, dass alle der folgenden Voraussetzungen erfüllt sind, bevor Sie Credant Server für Datensynchronisierungstasks und für das Sammeln gerätespezifischer Daten für den Datenschutz über den LANDesk Coreserver konfigurieren.

- Auf Ihrem Coreserver muss LANDesk Management Suite Version 9.5 installiert sein. (Diese Installation umfasst sowohl die Coreserversoftware als auch die unterstützende Datenbank.) Schrittweise Anleitungen zur Installation und Bereitstellung einer LANDesk Management Suite-Coreserver/Datenbankumgebung finden Sie auf der Website der Benutzercommunity des LANDesk Supports: LANDesk Benutzercommunity – Startseite
- Der LANDesk Standardagent (CBA, Common Base Agent) Version 9.5 muss für die verwalteten Geräte bereitgestellt werden, die Sie mit dem Extra "Datenschutz" schützen möchten.
- Ein oder mehrere Credant Enterprise Edition (CEE)-Server müssen in Ihrem Netzwerk eingerichtet und konfiguriert sein. Anweisungen zur Installation und Konfiguration eines Credant Servers finden Sie in der offiziellen Credant Dokumentation (siehe obiger Link).

Verwandte Themen

"Credant Data Protection" auf Seite 802

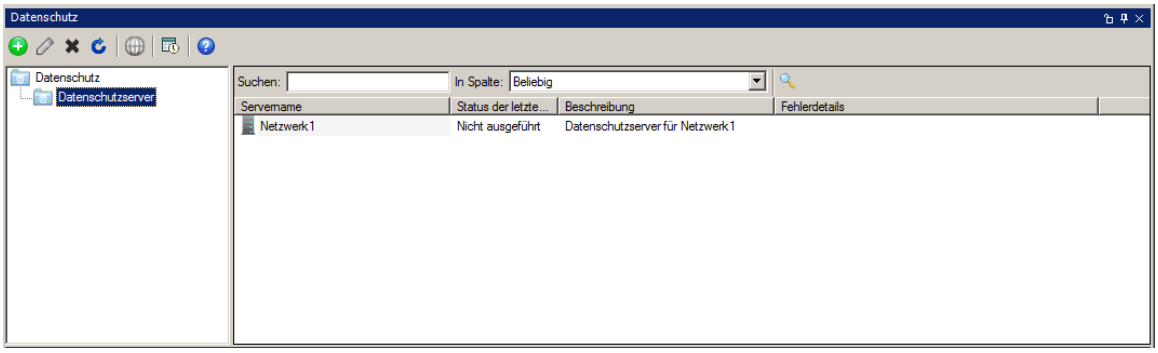
Verwenden des Extras "Datenschutz"

Mit dem integrierten Extra "Datenschutz" können Sie detaillierte Informationen zum Status der Datenintegrität von verwalteten Geräten in Ihrem LANDesk Management Suite-Netzwerk sammeln, speichern, verfolgen und anzeigen.

Das Fenster des Extras "Datenschutz"

Auf das Extra "Datenschutz" greifen Sie von der LANDesk Hauptkonsole aus über das Menü "Extras" (**Extras > Sicherheit und Compliance > Datenschutz**) oder über die Toolbox zu.

Im Fenster des Extras "Datenschutz" sind die Datenschutzserver aufgeführt, die Sie zu Ihrem Netzwerk hinzugefügt haben. (**HINWEIS:** Das Einrichten und Konfigurieren eines Datenschutzservers (Credant Enterprise-Servers) ist ein separater Task. Sie müssen bei der Einrichtung des Servers die Spezifikationen und Anweisungen des Anbieters befolgen. Anschließend können Sie den Server zu Ihrem LANDesk Netzwerk hinzufügen.)



Datenschutz-Symbolleiste

Das Fenster des Extras "Datenschutz" weist die folgenden Symbolleistenschaltflächen auf:

- **Neuer Datenschutzserver:** Hiermit können Sie einen vorhandenen Datenschutzserver zu Ihrem LANDesk Netzwerk hinzufügen bzw. so konfigurieren, dass dieser mit dem LANDesk Coreserver und der Datenbank kommunizieren und Informationen zu den Daten auf verwalteten Geräten senden kann, auf denen der Datenschutzagent installiert ist.
- **Eigenschaften:** Zeigt die Eigenschaftenseite für den ausgewählten Server an.
- **Löschen:** Entfernt den ausgewählten Datenschutzserver aus Ihrem LANDesk System.
- **Aktualisieren:** Lädt alle konfigurierten (hinzugefügten) Datenschutzserver neu mit den neusten Änderungen, die Sie vorgenommen haben.
- **Webkonsole (falls verfügbar):** Öffnet die Credant Webserveranwendung in einem Browser (wenn diese Software auf dem angegebenen Server im Rahmen der Konfiguration installiert wurde). Die Credant Webkonsole zeigt ausschließlich Credant spezifische Informationen an, aber keinerlei integrierte Inhalte von LANDesk. (**HINWEIS:** Zum Anzeigen des Webservers muss Silverlight installiert sein.)
- **Synchronisierungstask planen:** Erstellt einen geplanten Task, der Daten von ALLEN Datenschutzservern synchronisiert, die Sie in der LANDesk Konsole hinzugefügt/konfiguriert haben. Sie müssen keine separaten Tasks planen. Dieser Task wird mit einem Uhrzeit- und Datumsstempel versehen und zum Fenster "Geplante Tasks" hinzugefügt.
- **Hilfe:** Öffnet das LANDesk Help Center dort, wo sich die Hilfethemen zum Datenschutz befinden.

Verwandte Themen

"Info zum Datenschutzserver Seite "Servereigenschaften"" auf Seite 810

"Info zum Datenschutzserver: Seite "Datenbankverbindung"" auf Seite 811

Bereitstellen der Datenschutz-Agentensoftware für verwaltete Geräte

Dieses Hilfethema beschreibt, wie Sie die erforderliche Credant (Datenschutz)-Agentensoftware für Ihre verwalteten Geräte installieren bzw. bereitstellen. Sobald der Agent installiert ist, gilt das Gerät als geschützt. (Nähere Informationen finden Sie unter "Credant Data Protection" auf Seite 802).

Die Agentensoftware aktiviert den Datenschutz auf dem Gerät, die Sammlung von Datenschutzinformationen durch den LANDesk Coreserver sowie die sofortige Sammlung von Echtzeitdaten, mit denen die Konsolenansichten für das Inventar und die Übersicht aufgefüllt werden.

WICHTIG: Auf der Credant Website finden Sie Anweisungen zur Bereitstellung der Datenschutz-Agentensoftware
Wir empfehlen Ihnen, sich die in der offiziellen Credant Dokumentation beschriebenen Bereitstellungsverfahren für Agentensoftware anzusehen. Auf diese Dokumentation können Sie über die Credant Website zugreifen: Credant Enterprise Edition – Startseite.

Verwandte Themen

"Datenschutz – Voraussetzungen" auf Seite 804

"Verwenden des Extras "Datenschutz"" auf Seite 805

"Anzeigen von Datenschutzinformationen im Inventar" auf Seite 806

Anzeigen von Datenschutzinformationen im Inventar

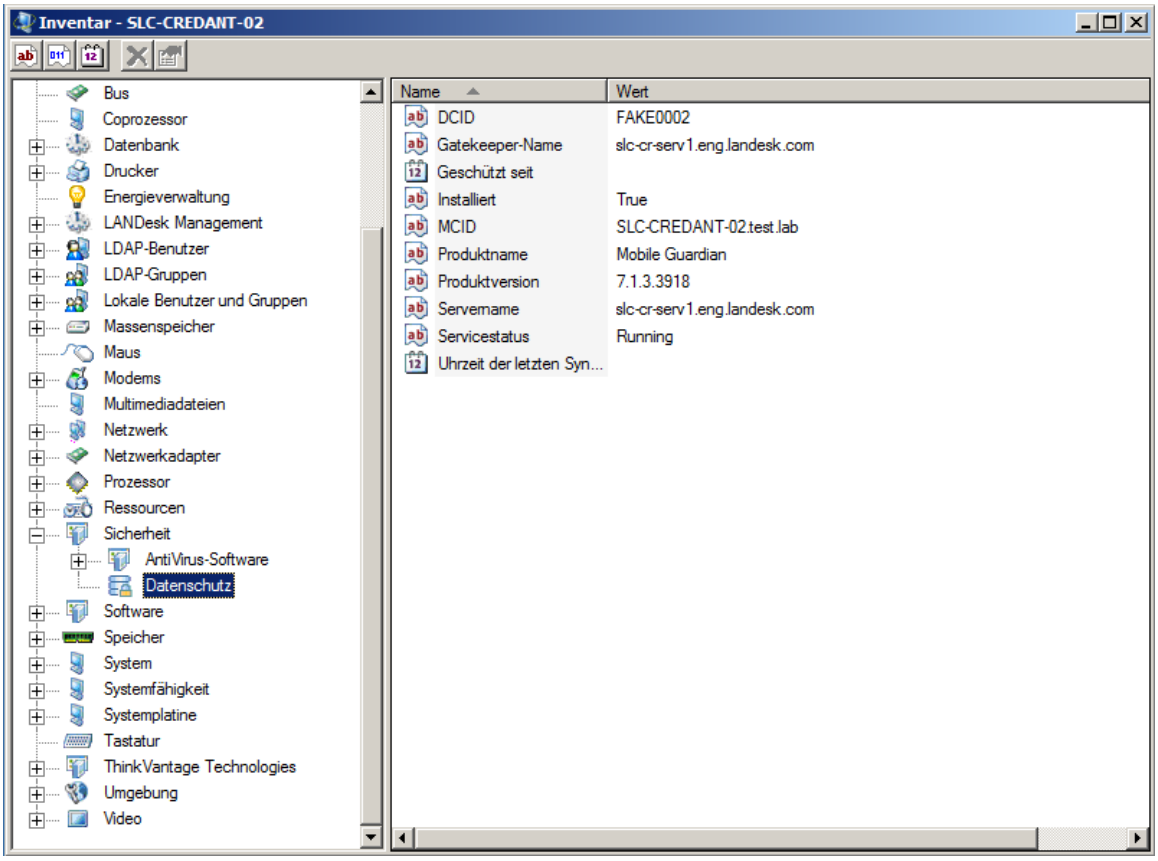
Sie können Datenschutzinformationen zu einem verwalteten Gerät in der LANDesk Inventaransicht anzeigen.

Anzeigen der Datenschutzinformationen in der Inventaransicht

So zeigen Sie die Datenschutzinformationen für ein Gerät an

1. Klicken Sie in der Konsole mit der rechten Maustaste auf das verwaltete Gerät, um auf das Kontextmenü zuzugreifen.
2. Klicken Sie auf **Inventar**, um die Inventaransicht zu öffnen.

3. Öffnen Sie die Komponente **Datenschutz** und überprüfen Sie, ob die Daten des Geräts geschützt sind.



Die Datenschutzkomponente umfasst die folgenden Attribute:

- **DCID:** Kennzeichnet das Gerät mit einem eindeutigen Kennungscode. Damit wird sichergestellt, dass die Synchronisierung zwischen der Datenschutz-Datenbank und der LDMS-Datenbank gültig und akkurat ist. Die DCID wird erst NACH dem ersten vollständigen Scan erstellt. Beim ersten Anzeigen weist sie unter Umständen noch keinen Wert auf; dieser wird aber ausgefüllt, nachdem der Datenschutzagent vollständig vom Inventarscanner gescannt wurde.
- **Gatekeeper-Name:** Liefert Informationen, die spezifisch für die Datenschutz-Datenbank sind.
- **Installiert:** Zeigt an, ob der Datenschutzagent auf dem verwalteten Gerät installiert ist oder nicht.
- **Uhrzeit der letzten Synchronisierung:** Zeigt die Uhrzeit der letzten Synchronisierung zwischen der Datenschutz-Datenbank und der LDMS-Datenbank an.
- **MCID:** Die von der Datenschutz-Agentenkonfiguration eingerichtete Hostkennung. Administratoren können diese Informationen zur Fehlersuche verwenden, wenn sie den Namen des Computers ändern, dieser Name sich hier aber nicht ändert.
- **Produktname:** Dies ist der Name des Datenschutzprodukts, der in der Registrierung des Geräts erscheint. Hier steht möglicherweise "Credant Mobile Guardian" oder "Mobile Shield". Das Feld soll dem dem Administrator Informationen über das Produkt an sich liefern.
- **Geschützt seit:** Zeigt das Datum an, an dem der Datenschutzagent auf dem verwalteten Gerät installiert wurde.

- **Servername:** Zeigt den Namen an, der beim Konfigurieren des Datenschutzservers eingegeben wurde, und mit dem dieser über die Konsole zu Ihrem LANDesk Netzwerk hinzugefügt wurde.
- **Produktversion:** Die durch die Headerdatei vom Installationsdienst bereitgestellte Versionsnummer.
- **Serverstatus:** Zeigt an, ob der Datenschutzdienst auf dem verwalteten Gerät ausgeführt wird. (**HINWEIS:** Diese Informationen werden vom Dienststeuerungs-Manager von Windows zusammengestellt.

Anzeigen der Datenschutzinformationen in der Echtzeitübersicht

Wenn der Datenschutzagent auf einem verwalteten Gerät installiert ist, können Sie die Übersichtsansicht über das Kontextmenü aufrufen. Sie liefert Ihnen sofort eine Echtzeitansicht der aktuellen Datenschutzinformationen für das ausgewählte Gerät.

So rufen Sie die Übersicht zu den Inventardaten auf

1. Klicken Sie mit der rechten Maustaste auf das ausgewählte Gerät.
2. Wählen Sie **Datenschutz - Übersicht** aus. (**HINWEIS:** Wenn der Datenschutzagent nicht installiert ist, steht diese Option nicht zur Verfügung.)
3. Zeigen Sie die Datenschutzinformationen für dieses Gerät an.

Der Übersichtsansicht enthält die folgenden Informationen:

- Gerätename
- DCID
- Geschützt seit
- Agentenversion
- Servername
- Gatekeeper
- Produktname
- Letztes Update

Verwandte Themen

"Generieren des Berichts zum Datenschutz" auf Seite 808

Generieren des Berichts zum Datenschutz

Das Extra "LANDesk Datenschutz" umfasst einen vordefinierten Bericht mit dem Namen "Bericht zum Datenschutz".

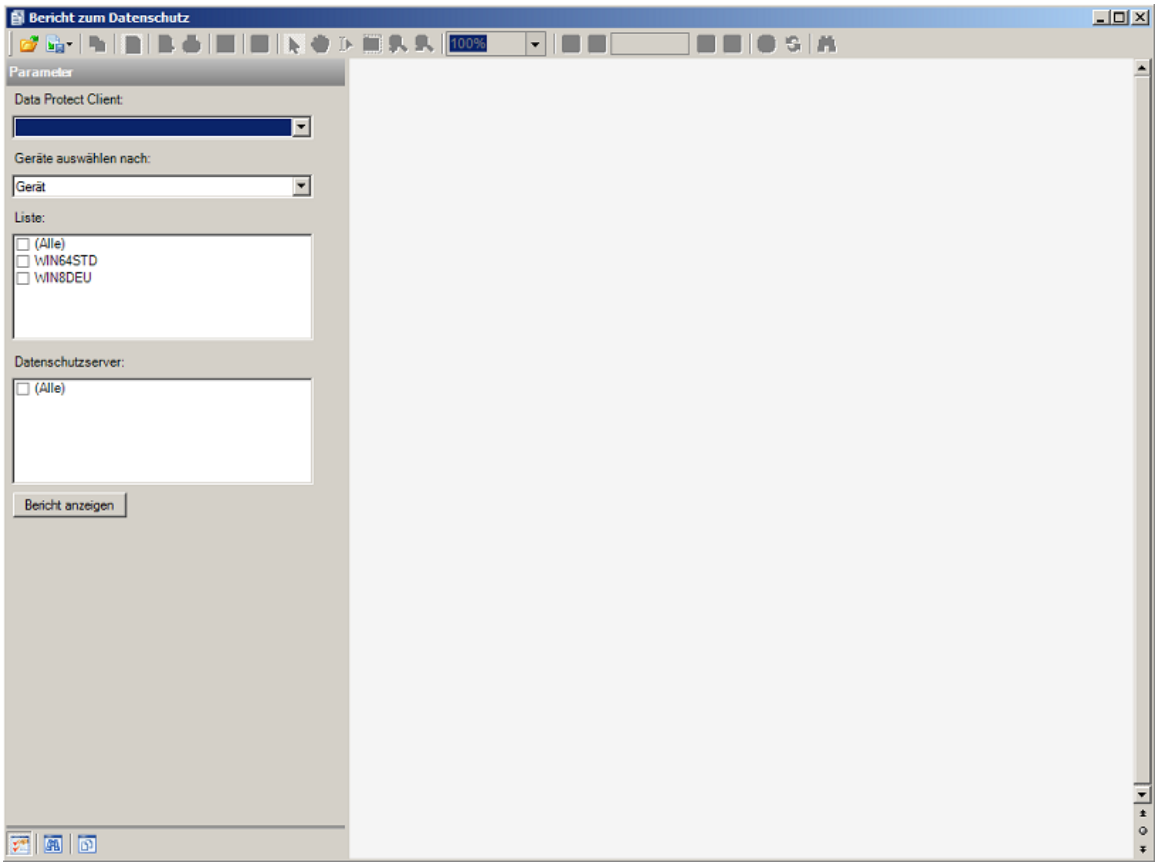
Der Bericht zum Datenschutz enthält die folgenden Informationen:

- geschützte Geräte
- auf den Geräten installierte Agenten (und Versionen)
- die verwendeten Credant Enterprise-Server

So generieren Sie den Bericht

1. Öffnen Sie in der LANDesk Konsole das Extra **Berichte**.
2. Klicken Sie auf **Alle Berichte** und wählen Sie den **Bericht zum Datenschutz**.

3. Doppelklicken Sie auf den **Bericht zum Datenschutz**, um den Bericht zu öffnen.



4. Geben Sie die von Ihnen gewünschten Parameter für den Bericht zum Datenschutz an.
5. Klicken Sie auf **Bericht anzeigen**.

6. Wenn Sie einen detaillierteren Bericht wünschen, klicken Sie auf eines der Diagramme im Bericht. Sie können aber auch zur zweiten Seite des Berichts gehen, um die detaillierte Textansicht anzuzeigen.

Verwandte Themen

"Anzeigen von Datenschutzinformationen im Inventar" auf Seite 806

Info zum Datenschutzserver Seite "Servereigenschaften"

Dieses Dialogfeld verwenden Sie zum Hinzufügen eines Datenschutzservers (der bereits gemäß den Anforderungen und Anweisungen für Credant Server installiert und konfiguriert wurde) zu Ihrer LANDesk Netzwerkumgebung. Der Datenschutzserver liefert dem LANDesk Coreserver Informationen zur Datenintegrität Ihrer verwalteten Geräten. Auf dem LANDesk Coreserver können Sie diese in der Inventaransicht und über das Extra "Berichte" einsehen.

Sie können einen oder mehrere Datenschutzserver verwenden.

Der konfigurierte Server stellt die Verbindung zwischen der Datenschutz-Datenbank und der LANDesk Coredatenbank her, die es Ihnen ermöglicht, Daten zwischen den Servern und den verwalteten "geschützten" Geräten in Ihrem Netzwerk zu synchronisieren. Der Server füllt dann die LANDesk Coredatenbank mit Informationen auf, die in der Inventaransicht und der Ansicht "Datenschutz - Übersicht" (mit Echtzeitaktualisierung) angezeigt werden können.

HINWEIS: ALLE Datenschutzserver werden gescannt
ALLE aufgeführten (konfigurierten/hinzugefügten) Datenschutzserver werden gescannt und die LANDesk Coredatenbank wird mit diesen Informationen aufgefüllt. Sie können keinen einzelnen Server angegeben. Sie können Server auch nicht einzeln synchronisieren. Gleichgültig wie viele Server in Ihrer Liste enthalten sind, sie werden alle durch den geplanten Task synchronisiert.

Diese Seite enthält folgende Optionen:

- **Servername:** Gibt den Datenschutzserver an, den Sie hinzufügen möchten. Sie können eine gültige IP-Adresse oder einen vollqualifizierten Domänenhostnamen für den gewünschten Server eingeben.
- **Beschreibung:** Geben Sie beliebige Informationen ein, die diesen Server von anderen Servern unterscheiden, die Sie eventuell noch hinzufügen.
- **Richtlinienproxyname:** Wird für eine Clientinstallation des Credant Agenten verwendet.
- **Port:** Gibt die vom Datenschutzserver verwendete Portnummer an, damit eine Datensynchronisierung mit der LANDesk Coredatenbank möglich ist.
- **Geräteserver-URL:** Gibt die Webadresse zum Starten der nativen Credant Webkonsole an.
- **Testen:** Verifiziert, ob die von Ihnen eingegebenen Serverinformationen einen gültigen Server in Ihrem Netzwerk darstellen.
- **Test abbrechen:** Beendet den Serververifizierungsprozess.
- **Speichern:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwandte Themen

"Info zum Datenschutzserver: Seite "Datenbankverbindung"" auf Seite 811

"Credant Data Protection" auf Seite 802

Info zum Datenschutzserver: Seite "Datenbankverbindung"

Diese Seite verwenden Sie zum Konfigurieren einer Verbindung zur Datenbank, die von dem Datenschutzserver verwendet wird, den Sie hinzufügen. In der Datenschutz-Datenbank werden Informationen zu den von Ihnen für die verwalteten Geräte festgelegten Datentypen gesammelt und in die LANDesk Coredatenbank übertragen.

HINWEIS: Eingegebene Informationen werden in Echtzeit aufgelöst
Die Informationen, die Sie auf dieser Seite in die Felder eingeben, werden in Echtzeit vom LANDesk Coreserver aufgelöst. Sie werden benachrichtigt, ob die Informationen gültig sind oder nicht.

Diese Seite enthält folgende Optionen:

- **Datenbankserver:** Der Name des Servers, der die Datenschutz-Datenbank hostet.
- **Datenbankname:** Der Name der Datenschutz-Datenbank.
- **Benutzername:** Geben Sie einen gültigen Benutzernamen für den Datenschutzserver ein, den Sie hinzufügen (konfigurieren) möchten.
- **Kennwort:** Geben Sie das Kennwort für den zuvor angegebenen Benutzernamen ein.
- **Testen:** Verifiziert, ob die von Ihnen eingegebenen Serverinformationen einen gültigen Server in Ihrem Netzwerk darstellen. (**HINWEIS:** Der Test beginnt automatisch, wenn Sie bei der Eingabe des Datenbankservers, dem Namen, dem Benutzernamen oder dem Kennwort eine Pause machen. Dies bedeutet, dass Sie nicht notwendigerweise auf die Schaltfläche "Test" klicken müssen.)
- **Test abbrechen:** Beendet den Serververifizierungsprozess.
- **Speichern:** Speichert die Änderungen und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwandte Themen

"Info zum Datenschutzserver Seite "Servereigenschaften"" auf Seite 810

"Credant Data Protection" auf Seite 802

LaunchPad Link-Manager

Informationen zu LaunchPad

LANDesk LaunchPad gibt Benutzern einen bestimmten Ausgangspunkt, von dem aus sie ihre physischen und virtuellen Anwendungen und URLs finden können. Mit LaunchPad geht die Zahl der Anrufe beim Help-Desk zurück, die sich auf die Installation von Anwendungen oder fehlende Symbole auf dem Desktop beziehen. LaunchPad liefert einer Gruppe von bekannten Benutzern (oder Geräten) eine Liste bekannter Anwendungen. Für Sie wird es damit überflüssig, manuell oder per Remotesteuerung von System zu System zu gehen, um anwendungsspezifische Probleme zu beseitigen.

LaunchPad hält Benutzer davon ab, Symbole zu löschen oder installierte Anwendungen durch unerwünschte Eingriffe unbrauchbar zu machen. Die Desktops von Endbenutzern werden automatisch mit neuen Anwendungen für bestimmte Gruppen aktualisiert. Benutzer können sich auf jedem beliebigen Gerät anmelden und ihre Links per Pull in den LaunchPad auf diesem Gerät ziehen lassen.

Sie können einen Verteilungspaket-Link erstellen, der die Installation einer Anwendung nahtlos mit deren Ausführung verknüpft (auch bekannt als Just-in-time-Link oder JIT-Link). Eine JIT-Linkdefinition wird auf der Konsole erstellt, indem als Linktyp "Verteilungspaket" ausgewählt und ein Softwareverteilungspaket mit diesem Link verknüpft wird.

Wenn ein JIT-Link in LaunchPad angezeigt und von einem Benutzer geöffnet wird, versucht die LANDesk Clientsoftware das damit verknüpfte Softwareverteilungspaket bereitzustellen, bevor die Zielanwendung ausgeführt wird. Beachten Sie, dass die Ziele von JIT-Links – im Gegensatz zu Linkzielen vom Typ "Ausführbare Datei" – selbst ausführbare Dateien sein müssen. LaunchPad löst Dateizuordnungen für JIT-Links nicht wie Dateizuordnungen für gewöhnliche Links auf.

Wenn das Paket erfolgreich bereitgestellt wurde, wird die ausführbare Zieldatei gestartet und der Link wird markiert, so dass die Bereitstellung in der Folge übersprungen und die ausführbare Datei direkt gestartet wird.

JIT-Links sind so konzipiert, dass der Endbenutzer den Installationsprozess nicht wahrnimmt. Daher sollten Softwareverteilungspakete, die den normalen Arbeitsfluss eines Endbenutzers unterbrechen, wie beispielsweise jene, die einen Neustart oder Benutzereingaben von erheblichem Umfang erfordern, oder eine außergewöhnlich lange Installationszeit haben, nicht mit JIT-Links verknüpft werden. Die Bereitstellung dieser Art von Softwareverteilungspaketen sollte entweder über das LANDesk Software-Verteilungsportal (bei dem der Benutzer den Zeitpunkt und die Art und Weise der Paketbereitstellung bestimmen kann) oder über eine Push-Standardverteilung außerhalb der üblichen Arbeitszeit erfolgen.

LaunchPad-Links, die keine JIT-Links sind, werden nicht im LaunchPad-Fenster angezeigt, wenn das Ziel nicht gefunden werden kann. Das bedeutet, dass Sie einen gewöhnlichen Link zu einer ausführbaren Datei oder einer später zu installierenden Datei erstellen können. Das Linksymbol erscheint erst dann im LaunchPad-Fenster, wenn das Ziel durch eine dieser alternativen Methoden erstellt wurde.

So öffnen Sie LaunchPad in Management Suite

1. Klicken Sie auf **Extras > Verteilung > LaunchPad Link-Manager**.

Spalten

- **Name:** Der Name des Links, wie er in den **Linkeigenschaften** definiert ist.
- **Beschreibung:** Die Beschreibung des Links, wie er in den **Linkeigenschaften** definiert ist.
- **Speicherort:** Wo sich der Link befindet (im LaunchPad, auf dem Desktop oder im Startmenü).

- **Kategorie:** Die Klassifikation des Links. Beispiele hierfür sind Links für Anwendungen oder Dienstprogramme oder Weblinks. Sie können Kategorien erstellen, die optimal auf die Anforderungen Ihrer Organisation zugeschnitten sind. In der Schnittstelle für die Endbenutzer wird jede Kategorie in einer separaten Zeile angezeigt.
- **Pfad:** Der Speicherort der mit dem Link verknüpften ausführbaren Datei.

Hinzufügen von Links zu LaunchPad

Elemente werden als Links zu LaunchPad hinzugefügt. Die Links (die als Symbole in LaunchPad angezeigt werden) können Anwendungen, Dienstprogramme, Links zu Webseiten usw. darstellen. Bevor die Links angezeigt werden können, müssen die folgenden Anweisungen befolgt werden.

Bei der Bereitstellung von LaunchPad-Links für einen Clientcomputer werden die Links erst dann auf dem Computer (auf dem Desktop, im Startmenü oder im LaunchPad-Fenster) angezeigt, wenn das Synchronisierungsprogramm der LANDesk Softwareverteilungsrichtlinie auf dem Computer ausgeführt wird. Das Richtliniensynchronisierungsprogramm kontaktiert beim Aufruf den LANDesk Core, fordert alle Updates einschließlich neuer LaunchPad-Links an und lädt diese herunter.

Normalerweise wird das Richtliniensynchronisierungsprogramm nach Plan in regelmäßigen Abständen auf den Clientcomputern ausgeführt. Administratoren können eine Richtliniensynchronisierung aber auch nach Belieben gemäß den nachstehend beschriebenen Verfahren ausführen. Alternativ hierzu kann es Benutzern gestattet werden, die Richtliniensynchronisierung selbst über einen LaunchPad-Link aufzurufen, wie nachstehend unter "So richten Sie einen Link für das Richtliniensynchronisierungsprogramm auf Clientcomputern ein" beschrieben.

So führen Sie die Richtliniensynchronisierung (policy.sync.exe) einmal auf einem Clientcomputer aus

1. Führen Sie den folgenden Befehl aus:

Bei einem 32-Bit-Betriebssystem:

```
"%ProgramFiles%\LANDesk\Shared Files\httpclient.exe" "http://localhost:9595/policy.cgi.exe?action=start"
```

Bei einem 64-Bit-Betriebssystem:

```
"%ProgramFiles(x86)%\LANDesk\Shared Files\httpclient.exe"
"http://localhost:9595/policy.cgi.exe?action=start"
```

So erzwingen Sie vom Core aus ein Synchronisierung auf einem Client

1. Öffnen Sie auf dem Core die Management Suite Konsole.
2. Klicken Sie auf **Extras > Verteilung > Skripte verwalten**.
3. Klicken Sie im linken Fensterbereich auf **Alle Skripte**.
4. Klicken Sie mit der rechten Maustaste auf das Skript "Package Sync" und klicken Sie dann auf **Planen**.
5. Ziehen Sie in der Netzwerkansicht den Client für die Synchronisierung auf den Task "Package Sync".
6. Klicken Sie mit der rechten Maustaste auf den Task "Package Sync" und klicken Sie dann auf **Eigenschaften**.
7. Wählen Sie auf der Seite **Task planen** im Feld **Für diese Geräte einen Plan erstellen** die Optionen **Jetzt starten** und **Alle Geräte** aus.

8. Klicken Sie auf **Speichern**. Daraufhin wird ein Skript ausgeführt, der die Richtliniensynchronisierung auf dem als Ziel definierten Client aufruft. Da Sie alle Geräte ausgewählt haben, können Sie, wenn Sie diesen Task in der Zukunft nochmals ausführen möchten, einfach auf der Seite **Task planen** auf **Jetzt starten** und dann auf **Speichern** klicken.

HINWEIS: Denken Sie daran, dass jedes mit diesem Skript angesprochene Gerät versuchen wird, Kontakt mit dem Core aufzunehmen und seine Richtlinien zu aktualisieren. Wenn Sie dieses Skript an eine große Zahl von Geräten gleichzeitig senden, kann dies den Coreserver belasten.

So richten Sie einen Link für das Richtliniensynchronisierungsprogramm auf Clientcomputern ein

1. Erstellen Sie in der LANDesk Konsole einen auf einer ausführbaren Datei basierenden LaunchPad-Link mit der Bezeichnung "Aktualisieren" und dem Ziel "%ProgramFiles%\LANDesk\Shared Files\httpclient.exe" "http://localhost:9595/policy.cgi.exe?action=start".
2. Klicken Sie mit der rechten Maustaste auf den Link und klicken Sie dann auf **Planen**.
3. Ziehen Sie in der Netzwerkansicht die Clients, an die die Bereitstellung erfolgen soll, auf den Task "Package Sync".
4. Klicken Sie mit der rechten Maustaste auf den Task und klicken Sie dann auf **Eigenschaften**.
5. Klicken Sie in den Fensterausschnitt **Task planen** und klicken Sie dann auf **Jetzt starten**. Der Link wird auf dem Clientcomputer angezeigt, sobald die nächste Richtliniensynchronisierung erfolgt.

So fügen Sie Links zu LaunchPad hinzu

1. Wenn LaunchPad nicht bereits geöffnet ist, klicken Sie auf **Extras > Verteilung > LaunchPad Link-Manager**.
2. Klicken Sie in der LaunchPad-Symbolleiste auf **Neuen Link hinzufügen**.
3. Klicken Sie auf die Seiten im linken Fensterausschnitt und füllen Sie die Felder im rechten Fensterausschnitt aus. Weitere Informationen zu den Feldern auf diesen Seiten finden Sie im nachstehenden Text. Wenn Sie fertig sind, klicken Sie auf **Speichern**.

Energieverwaltung

LANDesk® Power Manager – Übersicht

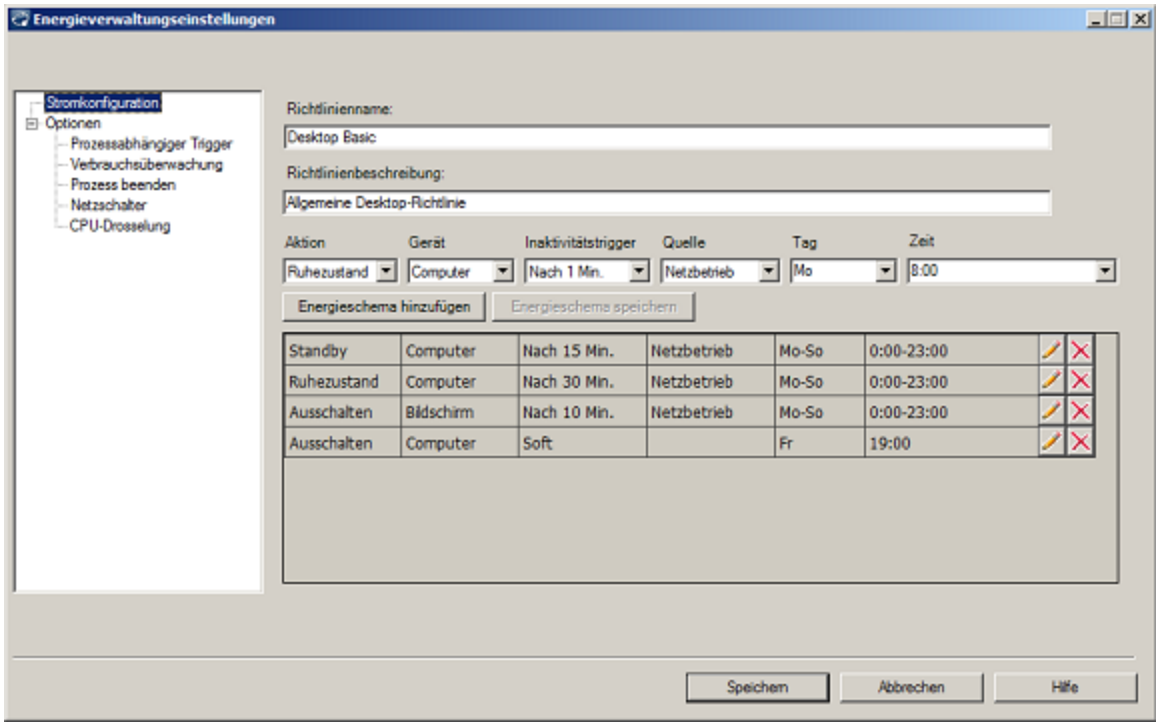
Mit dem Extra "LANDesk Energieverwaltung" können Sie den Stromverbrauch Ihrer verwalteten Computer von einem zentralen Ort aus überwachen. Sie können Richtlinien zur Energieverwaltung erstellen und bereitstellen und Berichte zur Bewertung der finanziellen Einsparungen und der Energieeinsparungen generieren. Ferner legen Sie die Bedingungen fest, unter denen Computer und Bildschirme in den Ruhezustand oder den Standby-Modus versetzt oder heruntergefahren werden.

Die Energieverwaltung besitzt eine Funktion, mit der Benutzer bestimmte Energieverwaltungsaktionen (wie z. B. "hartes" Herunterfahren oder Hard-Shutdown) durch die Verwendung einer clientseitigen Benutzerschnittstelle vermeiden können. Die so vermiedene Aktion findet dann statt, wenn die Richtlinie das nächste Mal auf diesem Computer ausgeführt oder aktualisiert wird.

Zur Funktionsweise

Der LANDesk Agent, der für jedes verwaltete Gerät bereitgestellt wird, umfasst eine Energieverwaltungsoption. Wenn Sie eine Energieverwaltungsrichtlinie für ein Gerät bereitstellen wollen, wird diese als Teil des Agenten aktiviert.

Sie definieren Richtlinien auf der Basis der spezifischen Anforderungen, die für verschiedene Typen von verwalteten Geräten gelten. Anschließend können Sie die Richtlinien für Gerätegruppen in Ihrem Unternehmen bereitstellen. Sie könnten beispielsweise eine Richtlinie für Server definieren, die ununterbrochen in Betrieb sein müssen, und eine zweite Richtlinie für Desktops, die typischerweise nicht während der Nacht und an Wochenenden genutzt werden.



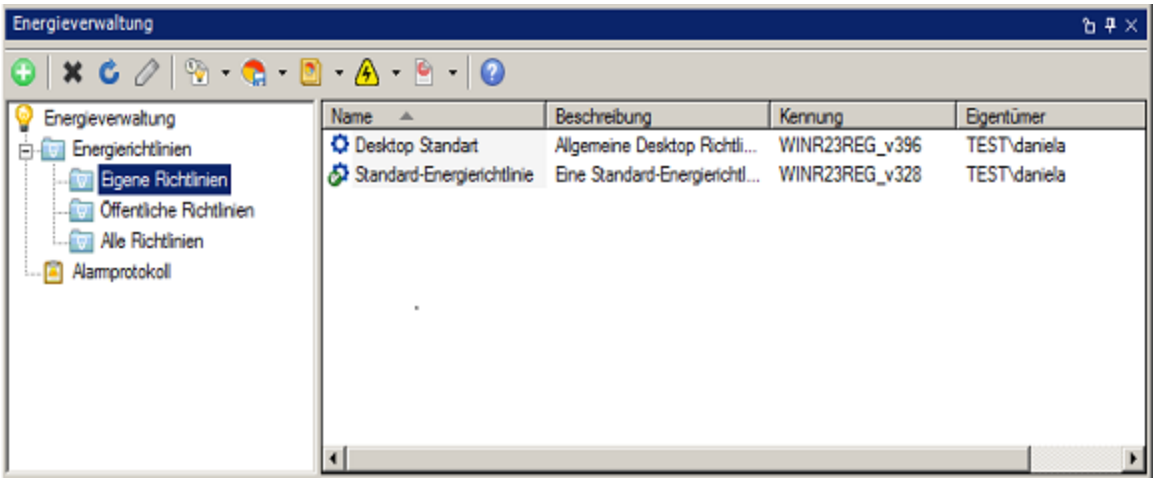
Jede Richtlinie enthält ein oder mehrere Energieschemas, d. h. bestimmte Regeln für energie- bzw. strombezogene Aktionen. Jedes Schema gilt während eines bestimmten Zeitraums für einen bestimmten Gerätetyp. Sie können zum Beispiel:

- Regeln für den Standby- oder Ruhezustand anwenden, die für Desktop- oder Laptop-Computer während der üblichen Arbeitszeiten gelten
- Schemas für Bildschirme definieren, die diese nach einer bestimmten Inaktivitätsdauer abschalten
- Schemas für Geräte definieren, die diese innerhalb bestimmter Tageszeiten automatisch einschalten

Arbeitet ein Benutzer an einem Computer, bei dem aufgrund einer Richtlinie jetzt normalerweise der Abschaltvorgang ansteht, wird der Benutzer über eine auf der Clientoberfläche angezeigte Nachricht davon in Kenntnis gesetzt und kann das Herunterfahren des Systems gegebenenfalls hinausschieben.

Schaltflächen der Symbolleiste "Energieverwaltung"

Das Extra "Energieverwaltung" umfasst eine Reihe von Schaltflächen, mit denen Sie verschiedene Energieverwaltungstasks ausführen können.



- **Neu:** Klicken Sie hierauf, um eine neue Energieverwaltungsrichtlinie zu erstellen.
- **Löschen:** Löscht die ausgewählte Energieverwaltungsrichtlinie.
- **Aktualisieren:** Aktualisiert die im linken Fensterbereich angezeigten Elemente.
- **Eigenschaften:** Zeigt die Eigenschaften der ausgewählten Energieverwaltungsrichtlinie an.
- **Planen:** Klicken Sie auf diese Schaltfläche, um die Bereitstellung der ausgewählten Energieverwaltungsrichtlinie zu planen.
- **Berichte:** Klicken Sie auf diese Schaltfläche, um einen Bericht mit Schätzwerten für die Energie- und Kosteneinsparungen zu erstellen, die Sie durch die Bereitstellung der ausgewählten Energieverwaltungsrichtlinie für eine bestimmte Gruppe von Geräten erzielen können. Sie können auch einen Bericht ausführen, der die Energie- und Kosteneinsparungen über einen festgelegten Zeitraum ausweist.
- **Vergangenheitsdaten:** Klicken Sie auf diese Schaltfläche, um Clientverbrauchsdaten für eine genauere Schätzung des Energieverbrauchs zusammenzutragen.

- **Anpassen:** Hier können Sie die Einstellungen anpassen, die den Gesamtstromverbrauch für bestimmte Hersteller und Computermodelle definieren.
- **Anwendungsverwaltung:** Hier können Sie die Prozesse verwalten, die bei der Anwendung einer Energierichtlinie aktiv sein können.

Erstellen einer Energieverwaltungsrichtlinie

Die Energieverwaltung verwendet richtlinienbasiertes Management, um Anweisungen zum Wechsel in den Standby-Modus, zum Herunterfahren oder zum Ein- und Ausschalten an Ihre verwalteten Computer zu senden. Sie erstellen Energieverwaltungsrichtlinien zur Steuerung bestimmter Computer und Computergruppen.

So erstellen Sie eine Energieverwaltungsrichtlinie

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Strukturansicht auf einen Richtlinienordner.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neu**.
4. Geben Sie einen Namen und eine Beschreibung für die Richtlinie ein.
5. Fügen Sie mindestens ein Energieschema zur Richtlinie hinzu. Wählen Sie in den sechs Listen (**Aktion**, **Gerät**, **Inaktivitätstrigger**, **Quelle**, **Tag** und **Zeit**) die gewünschten Einstellungen aus und klicken Sie auf **Energieschema hinzufügen**.

   Bei Bedarf können Sie mehrere Energieschemas hinzufügen. Um ein Energieschema aus einer Richtlinie zu entfernen, klicken Sie auf die Schaltfläche **Löschen** ( ) neben dem betreffenden Schema.
6. Erweitern Sie in der linken Spalte **Optionen**. Wählen Sie auf den sechs Seiten mit Optionen die gewünschten Einstellungen aus.
7. Wenn alle Optionen definiert sind, klicken Sie auf **Speichern**.

Klicken Sie hier, um Beschreibungen der Optionen für das Energieschema und die Energierichtlinie anzuzeigen.

Optionen für das Energieschema

- **Aktion:** Wählen Sie die auf den verwalteten Computern auszuführende Aktion aus (Ruhezustand, Standby, Einschalten, Ausschalten oder Alarm).
- **Gerät:** Wählen Sie das Gerät aus, auf dem die Aktion ausgeführt werden soll (z. B. Computer).
- **Inaktivitätstrigger:** Wählen Sie das Zeitintervall aus, das abgelaufen sein muss, bevor die Aktion getriggert wird (von 1 Minute bis 5 Stunden oder niemals). Hinweis: Wenn Sie in der Liste **Aktion** die Option **Ausschalten** auswählen, ändert sich der Titel dieser Liste von **Inaktivitätstrigger** in **Herunterfahren** (Hard oder Soft).
- **Quelle:** Wählen Sie die Energiequelle aus, die das Gerät verwendet (Netzbetrieb, Batteriebetrieb oder beides).
- **Tag:** Wählen Sie den Wochentag oder die Wochentage aus, an dem/denen die Aktion ausgeführt werden soll.
- **Zeit:** Wählen Sie die Tageszeit oder die Tageszeiten aus, an denen die Aktion ausgeführt werden soll.

Optionen für die Energierichtlinie

- **Optionen**: Bildschirmschoner deaktivieren, Lokale Reaktivierung aktivieren, Herunterfahren verzögern, Überwachen.
- **Prozessabhängiger Trigger**: Aktivieren Sie diese Option, um die Energierichtlinie zu verzögern, wenn einer der hier aufgeführten Prozesse erkannt wird. Die Richtlinie wird fortgesetzt, wenn nach der angegebene Anzahl von Minuten keine Prozesse erkannt wurden. Wenn Sie Prozesse zu dieser Liste hinzufügen möchten, verwenden Sie die Symbolleistenschaltfläche **Liste der prozessabhängigen Trigger**.
- **Verbrauchsüberwachung**: Aktivieren Sie diese Option, um die Energierichtlinie durchzusetzen, wenn die im Dialogfeld definierten Bedingungen erfüllt sind. Als Bedingungen können die CPU-Verwendung und der Netzwerkverkehr herangezogen werden. Wenn eine oder beide Bedingungen einen bestimmten Prozentschwellenwert unterhalb des Maximums erreichen, wird die Energierichtlinie durchgesetzt.
- **Prozess beenden**: Aktivieren Sie diese Option, um die in der Liste enthaltenen Prozesse während eines Herunterfahrens des Systems zu beenden. Wenn Sie Prozesse zu dieser Liste hinzufügen möchten, verwenden Sie die Symbolleistenschaltfläche **Liste der zu beendenden Prozesse**.
- **Netzschalter**: Aktivieren Sie diese Option, um die Aktionen zu konfigurieren, die bei der Betätigung von Netzschaltern durch den Benutzer bei einem verwalteten Gerät ausgelöst werden. Wählen Sie für jeden Schaltertyp die bei Netzbetrieb oder bei Akkubetrieb jeweils auszuführende Aktion aus. Für jede Situation kann eine Auswahl aus den folgenden Optionen getroffen werden: **Keine Aktionen ausführen**, **Energie sparen**, **Ruhezustand** oder **Herunterfahren**.
- **CPU-Drosselung**: Aktivieren Sie diese Option, um die CPU-Drosselung (zur Beschränkung des Stromverbrauchs der CPU) einer bereitgestellten Energierichtlinie zu konfigurieren. Wählen Sie jeweils eine Leistungsstufe für den Netzbetrieb und für den Akkubetrieb des Geräts aus. Folgende Leistungsstufen stehen zur Verfügung: **Höchste** (Minimum: 100, Maximum: 100), **Adaptive** (Minimum: 5, Maximum: 100), **Niedrig** (Minimum: 5, Maximum: 50) oder **Niedrigste** (Minimum: 5, Maximum: 33).

Verwenden der Aktion "Einschalten" mit Wake on LAN

Die Energieverwaltung verwendet Wake-on-LAN (WOL)-Technologie oder Intel vPro Wake up, um einen Computer zur Ausführung geplanter Tasks ferngesteuert einzuschalten. Damit die WOL-Funktionalität (d. h. die Remoteaktivierung über LAN) von der Energieverwaltung verwendet werden kann, müssen alle verwalteten Computer mit Netzwerkadaptern ausgestattet sein, die ordnungsgemäß konfiguriert sind und WOL unterstützen.

Die Energieverwaltung kann Ihnen die Aufgabe des Einrichtens und Konfigurierens der WOL-Funktionalität für Netzwerkadapter nicht abnehmen. Wenn die WOL-Funktionalität beim Netzwerkadapter eines Computers nicht aktiviert ist, kann eine Energieverwaltungsrichtlinie, deren Energieschema eine Aktion "Einschalten" umfasst, auf diesem Computer nicht erfolgreich ausgeführt werden. Die Energieverwaltung bietet derzeit keinerlei Möglichkeit, zu überprüfen, ob die WOL-Funktionalität eines Netzwerkadapters aktiviert ist oder nicht.

Verwenden der Funktion "Ruhezustand" unter Windows 2000 und Windows XP SP2

Die Energieverwaltung kann die Funktion "Ruhezustand" auf Computern mit Windows 2000 und Windows XP SP2 nicht automatisch aktivieren. Benutzer der von Ihnen verwalteten Computer müssen daher die Funktion "Ruhezustand" manuell wie folgt über die Systemsteuerung aktivieren.

1. Klicken Sie in der Systemsteuerung auf **Energieoptionen**.
2. Klicken Sie im Dialogfeld **Energieoptionen – Eigenschaften** auf die Registerkarte **Ruhezustand**.
3. Aktivieren Sie das Kontrollkästchen **Ruhezustand aktivieren** und klicken Sie auf **OK**.

Bereitstellen einer Energieverwaltungsrichtlinie

Im Anschluss an die Erstellung einer Richtlinie müssen Sie deren Ausführung auf einem verwalteten Gerät oder einer Gruppe von Geräten planen. Nach erfolgreichem Abschluss des Tasks ist die Energierichtlinie Teil des LANDesk Agenten auf den Zielgeräten und der Agent verwendet die in der Richtlinie festgelegten Energieschemas.

So stellen Sie eine Energieverwaltungsrichtlinie bereit

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Strukturansicht auf einen Richtlinienordner und wählen Sie die Richtlinie aus.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Planen** und wählen Sie **Richtlinie planen** aus.

   Das Extra **Geplante Tasks** wird geöffnet und die Energierichtlinie ist ausgewählt.
4. Verschieben Sie ein Gerät oder eine Gruppe aus der Netzwerkansicht auf die Richtlinie.
5. Klicken Sie mit der rechten Maustaste auf die Richtlinie und wählen Sie **Jetzt starten** aus.
6. Wenn Sie den Task zu einem anderen Zeitpunkt starten möchten, wählen Sie die Richtlinie aus, klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** und geben Sie die Startzeit für den Richtlinientask an.

Die Taskstatusbereiche zeigen an, bei welchen Geräten der Task erfolgreich abgeschlossen wurde. Wenn der Task auf irgendwelchen Geräten nicht abgeschlossen werden kann, wird die Fehlerursache angezeigt.

HINWEIS: Beim LANDesk Agenten auf den Zielgeräten muss die Energieverwaltung aktiviert worden sein, damit eine Energierichtlinie funktioniert. Wenn Sie eine Richtlinie bereitstellen und eine Fehlermeldung erhalten, die besagt, dass der Richtlinientask auf einem Gerät nicht gestartet werden kann, vergewissern Sie sich, dass die Energieverwaltung beim Agenten des Geräts aktiviert wurde.

Entfernen einer Energieverwaltungsrichtlinie

Sie können eine Energieverwaltungsrichtlinie von allen verwalteten Geräten oder von bestimmten Gerätegruppen entfernen. Dies geschieht mit Hilfe eines geplanten Tasks, der auf alle Geräte angewendet wird. Nach erfolgreichem Abschluss des Tasks ist die Energierichtlinie nicht mehr im LANDesk Agenten auf den Zielgeräten vorhanden.

So entfernen Sie eine Energieverwaltungsrichtlinie

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Planen** und wählen Sie **Energieverwaltung ausschalten** aus.

   Wenn Sie sich für die globale Option entscheiden, wird die Energieverwaltung von sämtlichen verwalteten Geräten entfernt.

   Wenn Sie sich für die Gruppenoption entscheiden, wählen Sie die Gerätegruppe oder Abfrage aus, für die Sie die Energieverwaltung entfernen möchten, und klicken Sie dann auf **OK**.
3. Klicken Sie im Extra "Geplante Tasks" mit der rechten Maustaste auf den Task **Energieverwaltung ausschalten** und klicken Sie auf **Jetzt starten**.
4. Wenn Sie den Task zu einem anderen Zeitpunkt starten möchten, wählen Sie den Task aus, klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** und geben Sie die Startzeit für den Ausschalttask an.

Die Taskstatusbereiche zeigen an, bei welchen Geräten der Task erfolgreich abgeschlossen wurde. Wenn der Task auf irgendwelchen Geräten nicht abgeschlossen werden kann, wird die Fehlerursache angezeigt.

Planen einer remoten Reaktivierung

Die Energieverwaltung plant einen Befehl "Einschalten" über das BIOS eines Geräts. Wenn das BIOS Reaktivierungs- bzw. Wakeup-Ereignisse nicht planen kann oder diese nicht über Windows planen kann, dann wird das Ereignis "Einschalten" nicht geplant. Wenn dies geschieht, haben Sie mehrere Möglichkeiten, das Problem zu lösen:

- Aktivieren Sie Plug-and-Play-Ereignisse im BIOS.
- Aktivieren Sie Ereignisse im BIOS.
- Aktualisieren Sie das Hersteller-BIOS.

Manche BIOS-Arten bieten gar keine Unterstützung für diese Funktion. In diesem Fall kann ein geplanter Task für Wake on LAN (WOL) zum Einschalten von Geräten zu einer bestimmten Zeit verwendet werden.

Wenn ein verwaltetes Gerät so konfiguriert wurde, dass Wake on LAN (WOL) oder Intel vPro Wake up verwendet wird, können Sie eine remote Reaktivierung planen, die das Gerät zur angegebenen Zeit einschaltet. Diese Funktion reaktiviert Geräte, die sich im Standby- oder Ruhezustand befinden sowie Geräte, die ausgeschaltet wurden.

Wenn sowohl WOL als auch Intel vPro Wake up aktiviert sind, wird zuerst die Intel vPro-Funktion ausgeführt und dann die WOL-Funktion.

So planen Sie eine remote Reaktivierung

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Planen** und wählen Sie **Remote Reaktivierung planen** aus.

   Das Extra **Geplante Tasks** wird geöffnet und der Task ist ausgewählt.
3. Verschieben Sie ein Gerät oder eine Gruppe aus der Netzwerkansicht auf den Task.
4. Klicken Sie mit der rechten Maustaste auf den Task und wählen Sie **Jetzt starten** aus.

5. Wenn Sie den Task zu einem anderen Zeitpunkt starten möchten, wählen Sie den Task aus, klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften** und geben Sie die Startzeit für den Task an.

Die Taskstatusbereiche zeigen an, bei welchen Geräten der Task erfolgreich abgeschlossen wurde. Wenn der Task auf irgendwelchen Geräten nicht abgeschlossen werden kann, wird die Fehlerursache angezeigt.

Verwalten von Anwendungen, die mit Energierichtlinien in Konflikt stehen

Auf verwalteten Geräten ausgeführte Anwendungen können unter Umständen mit den von Ihnen erstellten Energieverwaltungsrichtlinien in Konflikt stehen. Manche Anwendungen müssen weiterhin ausgeführt werden dürfen, selbst wenn die Energierichtlinie einen Befehl zum Herunterfahren des Geräts vorgibt. Andere Anwendungen dagegen dürfen die Durchsetzung der Richtlinie nicht stören und müssen im Rahmen des Ausschaltvorgangs beendet werden.

Das Alarmprotokoll der Energieverwaltung unterstützt Sie bei der Identifizierung der auf einem verwalteten Gerät ausgeführten Prozesse, die im Konflikt zu Energierichtlinien stehen können. Diese Konflikte werden mit dem Gerätenamen, der Uhrzeit und dem Namen des Prozesses protokolliert. Überprüfen Sie diese Protokolleinträge, um die Anwendungen zu bestimmen, die Konflikte verursachen.

Die Schaltfläche **Anwendungsverwaltung** ( ) in der Symbolleiste der Energieverwaltung umfasst drei Optionen, mit denen Sie potenzielle Konflikte mit Anwendungen regeln können:

- **Prozessabhängige Trigger angeben**: Prozesse, die Sie in diese Liste einschließen, dürfen selbst dann weiter ausgeführt werden, wenn die Energierichtlinie einen Befehl zum Herunterfahren vorgibt. Die Energierichtlinie wartet, bis die Prozesse beendet sind und fährt dann mit der Durchsetzung der Richtlinie fort.
- **Prozesse ermitteln, die beim Herunterfahren beendet werden sollen**: Prozesse, die Sie in diese Liste einschließen, können die Durchsetzung der Energierichtlinie stören und einen Zustand der "Schlaflosigkeit" (Insomnia) verursachen, bei dem das Gerät nicht heruntergefahren oder in den Standbymodus versetzt werden kann. Wenn diese Prozesse aktiv sind, werden Sie von der Energierichtlinie beendet, damit die Richtlinie weiter ausgeführt werden kann.
- **Zu ignorierende Prozesse**: Prozesse, die Sie in diese Liste einschließen, bedürfen keiner Aufmerksamkeit seitens der Energierichtlinie und müssen nicht in Alarmprotokolle eingeschlossen werden.

Anweisungen zur Verwendung dieser Optionen finden Sie in den folgenden Themen:

"Konfigurieren von Anwendungen, die nicht heruntergefahren werden sollten" auf Seite 821

"Konfigurieren von Anwendungen, die heruntergefahren werden sollten" auf Seite 822

"Konfigurieren von Anwendungen, die in Alarmprotokollen ignoriert werden sollen" auf Seite 823

Konfigurieren von Anwendungen, die nicht heruntergefahren werden sollten

Verwenden Sie die Symbolleistenschaltfläche **Prozessabhängige Trigger angeben**, um den Prozess eines beliebigen, wichtigen Programms zu beobachten und auf dessen Abschluss zu warten, bevor die Energierichtlinien durchgesetzt werden.

In manchen Umgebungen müssen Programme über einen längeren Zeitraum ausgeführt werden. Der Patchprozess der Management Suite kann beispielsweise wenig oder viel Zeit für die Installation der Patches in Anspruch nehmen. Wie viel Zeit für das Hochfahren eines verwalteten Geräts benötigt wird, ist im Prozess der Patchbereitstellung eine unbekannte Größe. Bei anderen Programmen in einer Umgebung können ähnliche Parameter und Prozesse gegeben sein, die keinesfalls unterbrochen werden dürfen.

So identifizieren Sie Anwendungen, die nicht heruntergefahren werden sollten

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anwendungsverwaltung** und wählen Sie **Prozessabhängige Trigger angeben**.
3. Fügen Sie Prozessnamen zur Liste hinzu, ändern oder löschen Sie diese.
4. Wenn die Liste fertiggestellt ist, klicken Sie auf **OK**.

HINWEIS: Die Liste, die Sie hier erstellen, wird nur dann für ein verwaltetes Gerät übernommen, wenn Sie in der Energieverwaltungsrichtlinie für das betreffende Gerät die Option **Prozessabhängiger Trigger** aktiviert haben.

Klicken Sie hier, um eine Beschreibung der Optionen im Dialogfeld **Liste der prozessabhängigen Trigger** anzuzeigen.

- **Hinzufügen:** Fügt einen Prozess hinzu, bei dem es sich um eine bekannte .exe-Datei handelt, für die die Energierichtlinie verzögert werden muss.
- **Importieren:** Fügt einen Prozess aus Informationen hinzu, die unter Verwendung der Vergangenheitsdaten von Clientgeräten erfasst wurden. Hiermit werden Prozesse eingeschlossen, die im Alarmprotokoll der Energieverwaltung aufgeführt sind.
- **Löschen:** Entfernt den ausgewählten Prozess aus dieser Liste.
- **Ändern:** Klicken Sie auf diese Schaltfläche, um den Namen der .exe-Datei zu ändern.
- **Alle:** Wählt alle Prozesse in der Liste aus.
- **Keine:** Löscht alle in der Liste enthaltenen Prozesse.

Konfigurieren von Anwendungen, die heruntergefahren werden sollten

Die Symbolleistenschaltfläche **Prozesse ermitteln, die beim Herunterfahren beendet werden sollen** verwenden Sie, um Prozesse zu beenden, die bei einer Energierichtlinienoption zu einer Verzögerung führen könnten. Manche Prozesse führen dazu, dass ein Gerät die in den Energierichtlinien konfigurierten Parameter nicht einhält. Der gleiche Prozess wirkt sich auf einige oder auf viele Geräte aus, die die Richtlinie befolgen. Die Energieverwaltung beendet die Prozesse, die das Gerät daran hindern können, in den Ruhezustand zu wechseln oder herunterzufahren.

So identifizieren Sie Anwendungen, die beim Herunterfahren eines Systems beendet werden sollten

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anwendungsverwaltung** und wählen Sie **Prozesse ermitteln, die beim Herunterfahren beendet werden sollen**.
3. Fügen Sie Prozessnamen zur Liste hinzu, ändern oder löschen Sie diese.
4. Wenn die Liste fertiggestellt ist, klicken Sie auf **OK**.

HINWEIS: Die Liste, die Sie hier erstellen, wird nur dann für ein verwaltetes Gerät übernommen, wenn Sie in der Energieverwaltungsrichtlinie für das betreffende Gerät die Option **Liste der zu beendenden Prozesse** aktiviert haben.

Klicken Sie hier, um eine Beschreibung der Optionen im Dialogfeld **Liste der zu beendenden Prozesse** anzuzeigen.

- **Hinzufügen:** Fügt einen Prozess hinzu, bei dem es sich um eine bekannte .exe-Datei handelt, die beendet werden muss.
- **Importieren:** Fügt einen Prozess aus Informationen hinzu, die unter Verwendung der **Vergangenheitsdaten** von Clientgeräten erfasst wurden. Hiermit werden Prozesse eingeschlossen, die im Alarmprotokoll der Energieverwaltung aufgeführt sind.
- **Löschen:** Entfernt den ausgewählten Prozess aus dieser Liste.
- **Ändern:** Klicken Sie auf diese Schaltfläche, um den Namen der .exe-Datei zu ändern.
- **Alle:** Wählt alle Prozesse in der Liste aus.
- **Keine:** Löscht alle in der Liste enthaltenen Prozesse.

Konfigurieren von Anwendungen, die in Alarmprotokollen ignoriert werden sollen

Die Symbolleistenschaltfläche **Zu ignorierende Prozesse in Ausnahmeprotokollen angeben** verwenden Sie, um die Prozesse zu bestimmen, die von der Energierichtlinie nicht berücksichtigt werden müssen. Durch das Hinzufügen von Prozessen zu dieser Liste verringert sich der Umfang der Protokolldateien, die im Zusammenhang mit der Energieverwaltung generiert werden. So können Sie sich besser auf die Anwendungen konzentrieren, die im Hinblick auf die Überwachung von Problemen mit der Energieverwaltung von Interesse sind.

So identifizieren Sie Anwendungen, die in Alarmprotokollen ignoriert werden können

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anwendungsverwaltung** und wählen Sie **Zu ignorierende Prozesse in Ausnahmeprotokollen angeben**.
3. Fügen Sie Prozessnamen zur Liste hinzu, ändern oder löschen Sie diese.
4. Wenn die Liste fertiggestellt ist, klicken Sie auf **OK**.

Klicken Sie hier, um eine Beschreibung der Optionen im Dialogfeld **Zu ignorierende Prozesse** anzuzeigen.

- **Hinzufügen:** Fügt einen Prozess hinzu, bei dem es sich um eine bekannte .exe-Datei handelt, die ignoriert werden kann.
- **Importieren:** Fügt einen Prozess aus Informationen hinzu, die unter Verwendung der **Vergangenheitsdaten** von Clientgeräten erfasst wurden. Hiermit werden Prozesse eingeschlossen, die im Alarmprotokoll der Energieverwaltung aufgeführt sind.
- **Löschen:** Entfernt den ausgewählten Prozess aus dieser Liste.
- **Ändern:** Klicken Sie auf diese Schaltfläche, um den Namen der .exe-Datei zu ändern.

Anzeigen von Energieverwaltungsberichten

Mit dem Extra "Energieverwaltung" können Sie Berichte zu Energie- und Kosteneinsparungen sowie Berichte mit Verlaufsdaten erstellen und anzeigen. Berichte umfassen zusammengefasste Berechnungen der Energie- oder Kosteneinsparungen. Die Grundlage hierfür bilden die geschätzten Energiekosten und eine durchschnittliche aktive Nutzung der ausgewählten Computer, die Sie mit einem Bericht verknüpfen.

Es gibt zwei verschiedene Arten von Einsparungsberichten:

- **Stromverbrauch**: Vergleicht die Anzahl der verbrauchten kWh (Kilowattstunden) bei Anwendung von Energieverwaltungsrichtlinien mit der Verbrauchszahl ohne Anwendung einer Energieverwaltungsrichtlinie.
- **Finanzielle Einsparungen**: Liefert eine Schätzung der Kosteneinsparungen, die bei der Anwendung von Energieverwaltungsrichtlinien erreicht werden können.

Die Einsparungen können auf Tages-, Wochen-, Monats- oder Jahresbasis berechnet werden. Wenn Sie Vergangenheitsdaten gesammelt haben, können Sie Berichte desselben Typs für die Vergangenheit ausführen.

Wie Berichte erstellt werden

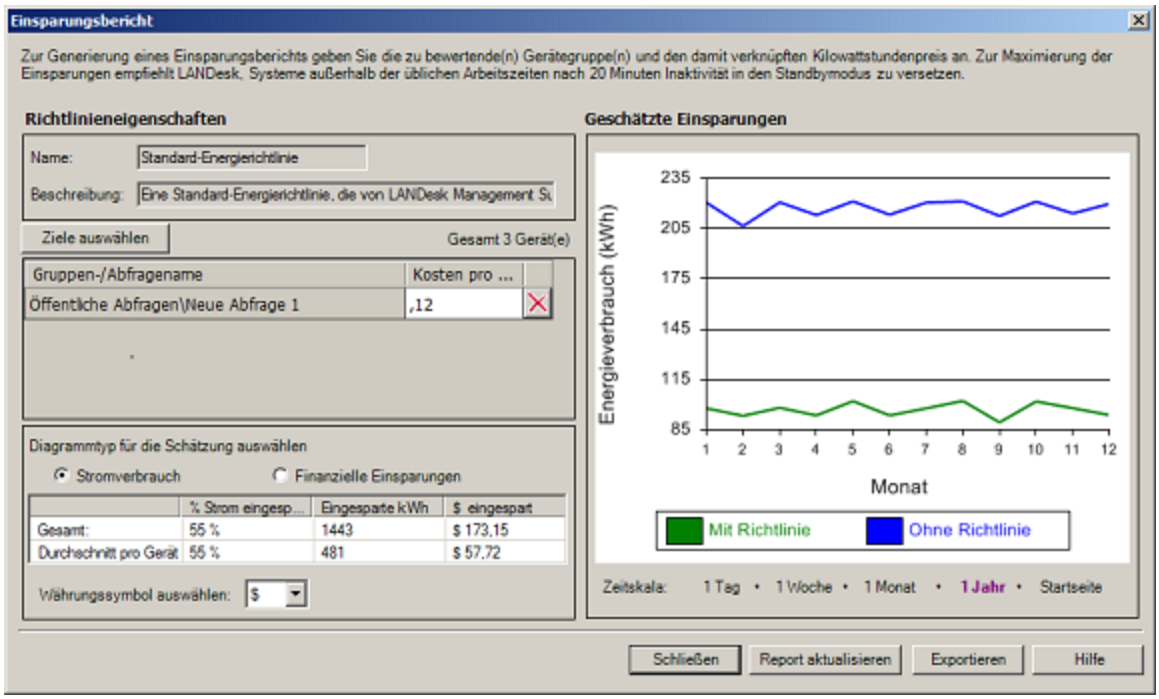
Energieverwaltungsprozesse auf verwalteten Geräten verfolgen die Zeiten, in denen jedes einzelne Gerät aktiv verwendet wird. Berichte werden auf der Basis einer XML-Datei erstellt, in der Informationen zur Nutzung gesammelt und eine durchschnittliche Nutzungsdauer für die Computer berechnet wird.

Jedes Mal, wenn Sie einen Bericht ausführen, wählen Sie einzelne Geräte oder Gerätegruppen aus. Der Bericht sammelt dann Daten zu diesen Geräten und gibt sie in Form einer Zusammenfassung der Nutzungsdaten aus. Die Stunden des Gebrauchs werden entweder mit dem durchschnittlichen Stromverbrauch des Gerätetyps multipliziert (für Berichte zum Stromverbrauch) oder den geschätzten Einsparungen, wenn das Gerät heruntergefahren bleibt (für Berichte zu den finanziellen Einsparungen).

Die folgenden Elemente haben einen Einfluss auf die Berechnungen in Berichten. Sie können jedes dieser Elemente ändern, um die Berichte auf Ihre speziellen Gegebenheiten zuzuschneiden.

- **Kosten pro kWh**: Als Standardwert wird ein standardmäßiger Durchschnitt verwendet. Wenn Sie die tatsächlichen Kosten pro kWh Ihrer Stromabrechnung kennen, ändern Sie den Wert entsprechend.
- **Benutzerdef. Stromverbrauchseinstellungen**: Für Berichte werden standardmäßig die durchschnittlichen Verbrauchseinstellungen für Desktops und Laptops verwendet. Wenn Sie spezifischere Daten verwenden möchten, können Sie auf Daten für bestimmte Hersteller und Modelle zurückgreifen.
- **Clientverbrauchsdaten**: Für Berechnungen wird standardmäßig ein durchschnittlicher Tagesverbrauch für Clients verwendet. Wenn Sie spezifischere Daten verwenden möchten, können Sie Vergangenheitsdaten von Ihren verwalteten Geräten für die Berichtsberechnungen einsetzen.

Wenn Sie einen Bericht zu den Einsparungen ausführen, verwenden Sie das folgende Dialogfeld zur Auswahl der Optionen und um eine Vorschau der Ergebnisse anzuzeigen.



Ausführen eines Energieverwaltungsberichts

Wenn Sie Berichte zu Energieeinsparungen und Verlaufsberichte ausführen möchten, verwenden Sie die Schaltfläche **Berichte** der Symbolleiste "Energieverwaltung".

HINWEIS: Damit Berichte generiert werden können, müssen Sie in der Netzwerkansicht zunächst Computergruppen mit mindestens einem Gerät oder Abfragen erstellen. Zur Auswahl der Geräte, die in Berichte enthalten sein sollen, verwenden Sie Gruppen und Abfragen.

So führen Sie einen Energieverwaltungsbericht aus

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Strukturansicht auf einem Richtlinienordner und wählen Sie die Richtlinie aus, für die Sie den Bericht ausführen möchten.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Berichte** und wählen Sie **Einsparungsbericht** oder **Verlaufsbericht** aus.
4. Klicken Sie auf **Ziele auswählen**. Wählen Sie die Gruppen oder Abfragen für die Geräte aus, die in den Bericht eingeschlossen werden sollen. Klicken Sie auf **OK**.

   Die von Ihnen ausgewählten Elemente werden mit den zugehörigen Kosten pro kWh aufgeführt. Die Gesamtzahl der Geräte in der Gruppe wird ebenfalls angezeigt.
5. Wenn Sie die Berechnung anhand von anderen Kosten pro kWh durchführen möchten, ändern Sie einfach den Zahlenwert im Feld **Kosten pro kWh**. Um eine Gruppe oder Abfrage: aus dem Bericht zu entfernen, klicken Sie auf die zugehörige Schaltfläche **Löschen**. Klicken Sie auf **Bericht aktualisieren**, um das Diagramm zu aktualisieren, wenn Ihre Änderungen abgeschlossen sind.
6. Wählen Sie einen Diagrammtyp aus ("Stromverbrauch" oder "Finanzielle Einsparungen").

7. Wählen Sie das Währungssymbol aus, das im Bericht verwendet werden soll.
8. Wählen Sie unterhalb des Diagramms den Zeitrahmen für den Bericht aus (von 1 Tag bis zu 1 Jahr).
9. Wenn Sie eine Kopie des Berichts exportieren möchten, klicken Sie auf **Exportieren** und geben Sie einen Speicherort für die Datei an.

HINWEIS: Wenn Sie einen Verlaufsbericht ausführen möchten, müssen Sie zunächst Vergangenheitsdaten für verwaltete Geräte gesammelt haben (über die Schaltfläche **Vergangenheitsdaten** der Symbolleiste. Wenn keine Vergangenheitsdaten vorliegen, wird kein Diagramm von der Berichtsfunktion erstellt und es wird auch keine Berichtsdatei exportiert.

Verwenden von Vergangenheitsdaten für Stromverbrauchsberichte

Sie können Stromverbrauchsdaten für verwaltete Geräte sammeln, wenn Sie Berichte erstellen möchten, die den tatsächlichen Stromverbrauch eines Geräts über einen bestimmten Zeitraum darstellen. Diese Daten werden in der Datenbank gespeichert und verwendet, sobald Sie einen Bericht ausführen, der die Geräte einschließt, für die Sie Daten sammeln.

Die Symbolleistenschaltfläche **Vergangenheitsdaten** verwenden Sie zum Starten und Stoppen der Datensammlung oder zum Löschen von Daten aus der Datenbank.

Nachdem Sie die Clientverbrauchsdaten gesammelt haben, können Sie Standardverbrauchsdaten für Clients durch tatsächliche Vergangenheitsdaten ersetzen, die Sie für Ihre verwalteten Geräte gesammelt haben.

So ersetzen Sie den angenommenen Stromverbrauch durch Vergangenheitsdaten

1. Klicken Sie in der Symbolleiste "Energieverwaltung" auf die Schaltfläche **Anpassen** und wählen Sie **Angenommenen Clientverbrauch durch Vergangenheitsdaten ersetzen**.
2. Wählen Sie die Gruppen oder Abfragen aus, für die Sie Vergangenheitsdaten verwenden möchten.
3. Wählen Sie einen Zeitraum für die Daten aus – entweder die letzte Woche oder einen anderen Zeitraum.
4. Klicken Sie auf **Standardverbrauchstabelle generieren**.

Die neuen Daten werden zum Generieren von Berichten verwendet. Sie ersetzen die durchschnittlichen Verbrauchsdaten, die standardmäßig für die Schätzung der Einsparungen verwendet werden.

Verwandte Themen

Anweisungen zur Verwendung der Optionen für Vergangenheitsdaten finden Sie in den folgenden Themen:

"Sammeln von Clientverbrauchsdaten" auf Seite 827

"Alte Clientverbrauchsdaten löschen" auf Seite 827

Sammeln von Clientverbrauchsdaten

So sammeln Sie Clientverbrauchsdaten:

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Vergangenheitsdaten** und wählen Sie eine Aktion aus (**Sammlung von Clientverbrauchsdaten starten** oder **Sammlung von Clientverbrauchsdaten stoppen**).

   Im Fenster **Geplante Tasks** wird ein mit dem Datum und der Uhrzeit gekennzeichneter Task geöffnet.
3. Verschieben Sie einzelne Geräte, Gruppen oder Abfragen mit Ziehen und Ablegen aus der Netzwerkansicht auf den Task.
4. Wenn Sie den Task jetzt starten wollen, klicken Sie mit der rechten Maustaste darauf und wählen Sie **Jetzt starten** aus.
5. Wenn Sie den Task für die Ausführung zu einem späteren Zeitpunkt planen wollen, wählen Sie den Task aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Eigenschaften**. Klicken Sie auf **Task planen > Später starten** und wählen Sie die gewünschten Zeitplanoptionen aus.

Die beiden Bereiche im Extra "Geplante Tasks" zeigen den Taskfortschritt an sowie die Geräte, für die der Task nicht abgeschlossen werden konnte und den jeweiligen Grund.

Alte Clientverbrauchsdaten löschen

So löschen Sie alte Clientverbrauchsdaten aus der Datenbank

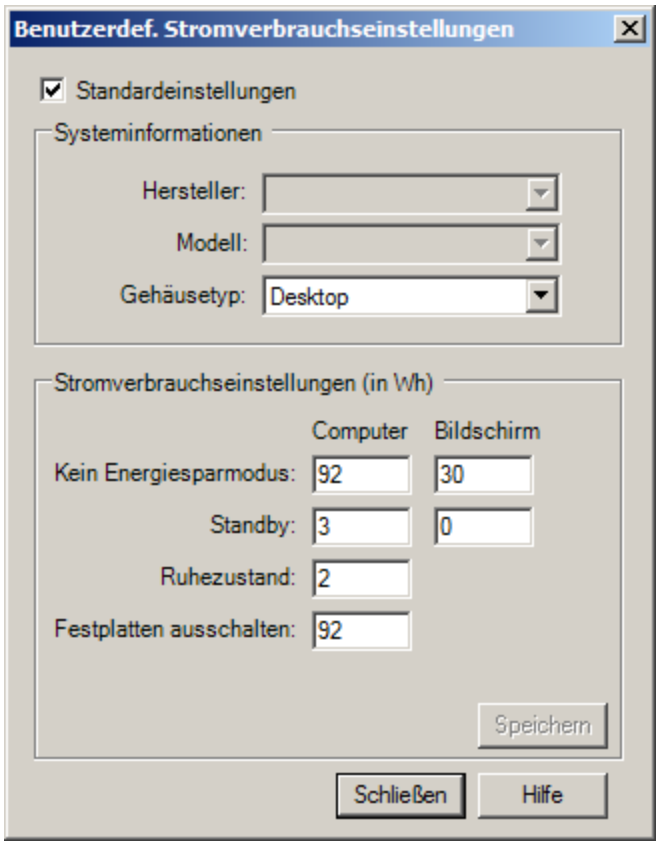
Nachdem Sie über einen gewissen Zeitraum hinweg Daten gesammelt und zur Erstellung von Berichten verwendet haben, werden Sie unter Umständen die alten Daten in der Datenbank löschen wollen. Damit wird sichergestellt, dass die Vergangenheitsdaten aus der jüngsten Vergangenheit stammen.

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Vergangenheitsdaten** und wählen Sie **Alte Clientverbrauchsdaten löschen** aus.
3. Geben Sie ein Datum ein und klicken Sie auf **Löschen**.

Vergangenheitsdaten zum Energieverbrauch und zur Stromverwendung vor dem angegebene Datum werden aus der Datenbank gelöscht.

Anpassen der Stromverbrauchseinstellungen

Das Extra "Energieverwaltung" umfasst ein Dienstprogramm, mit dem Sie die Stromverbrauchseinstellungen für ähnliche Computer zur präziseren Berichterstattung über die Energieverwaltung anpassen können. Die von Ihnen in diesem Dialogfeld ausgewählten und erstellten Einstellungen werden zur Berechnung von Berichtsdaten verwendet.



Standardeinstellungen

Die im Dialogfeld **Benutzerdefinierte Stromverbrauchseinstellungen** angezeigten Standardeinstellungen basieren auf dem Computertyp, auf den sich ein bestimmter Bericht bezieht.

Bei einem Desktop-Computer basieren die angezeigten Standard-Stromverbrauchseinstellungen auf den durchschnittlichen Einstellungen eines typischen Desktop-Computers. Bei Laptop-Computern sind die Standardeinstellungen niedriger, da Laptops in der Regel weniger Strom verbrauchen.

So ändern Sie die Standardeinstellungen für den Stromverbrauch

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anpassen** ( ) und wählen Sie **Benutzerdef. Stromverbrauchseinstellungen** aus.
3. Wählen Sie den **Gehäusetyp** aus (Desktop oder Laptop).
4. Ändern Sie die Stromverbrauchseinstellungen in den Feldern unter **Computer** und definieren Sie den Stromverbrauch für die verschiedenen Energiezustände des Gehäusetyps.
5. Ändern Sie die Stromverbrauchseinstellungen in den Feldern unter **Bildschirm** und definieren Sie den Stromverbrauch für die beiden Bildschirmenergiezustände **Kein Energiesparmodus** und **Standby**

Benutzerdefinierte Einstellungen für bestimmte Modelle

Sie können vorkonfigurierte benutzerdefinierte Einstellungen verwenden, die der von Ihnen verwendeten Art von Ausrüstung entsprechen. Zur Arbeitserleichterung wurden Energieeinstellungen für eine Vielzahl von populären Desktop- und Laptop-Computerherstellern integriert.

Wenn Sie beispielsweise den Energieverbrauch bei einem Desktop-Computer vom Typ "Dell Inspiron 531s" überwachen wollen, wählen Sie in der Dropdownliste **Hersteller** den Eintrag **Dell Inc.** aus und in der Dropdownliste **Modell** den Eintrag **Inspiron 531s**. Die Stromverbrauchseinstellungen für den Computer und den zugehörigen Bildschirm wurden auf der Basis von Daten erstellt, die sich aus einem LANDesk Bestand für einen Computer vom Typ "Inspiron 531s" ergaben.

So fügen Sie Stromverbrauchseinstellungen für spezifische Hardwaremodelle hinzu

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anpassen** ( ) und wählen Sie **Benutzerdef. Stromverbrauchseinstellungen** aus.
3. Deaktivieren Sie das Kontrollkästchen **Standardeinstellungen**.
4. Wählen Sie den **Hersteller** und das **Modell** für den Gerätetyp aus, den Sie verwenden möchten.
5. Klicken Sie auf **Schließen**, um die Daten für dieses Modell zu speichern.
6. Wiederholen Sie die Schritte 2 bis 4 für jedes Modell, das Sie in die Berechnungen des Stromverbrauchs einbeziehen möchten.

Die von Ihnen gespeicherten Stromverbrauchseinstellungen werden gegen die verwalteten Geräte abgeglichen, die Sie in die Berichterstellung einschließen.

Benutzerdefinierte Einstellungen für sonstige Modelle

Wurde das Kontrollkästchen **Standardeinstellungen** markiert, zeigen die Felder für die Stromverbrauchseinstellungen den durchschnittlichen Stromverbrauch eines typischen Desktop- oder Laptop-Computers an. Wenn Sie das Kontrollkästchen **Standardeinstellungen** deaktivieren, können Sie diese Felder dazu verwenden, Stromverbrauchseinstellungen für bestimmte Marken und Modelle einzugeben, die nicht bereits in den Listen für Hersteller und Modell enthalten sind.

So fügen Sie Stromverbrauchseinstellungen für sonstige Hardwaremodelle hinzu

Wenn die Art der Ausrüstung, die Sie verwalten möchten, nicht in den vorkonfigurierten Dropdownlisten mit **Systeminformationen** aufgeführt ist, können Sie die von Ihnen benötigten Informationen manuell eingeben. Damit Sie akkurate Ergebnisse erhalten, sollten Sie die Verbrauchsdaten laut Angaben des Herstellers übernehmen.

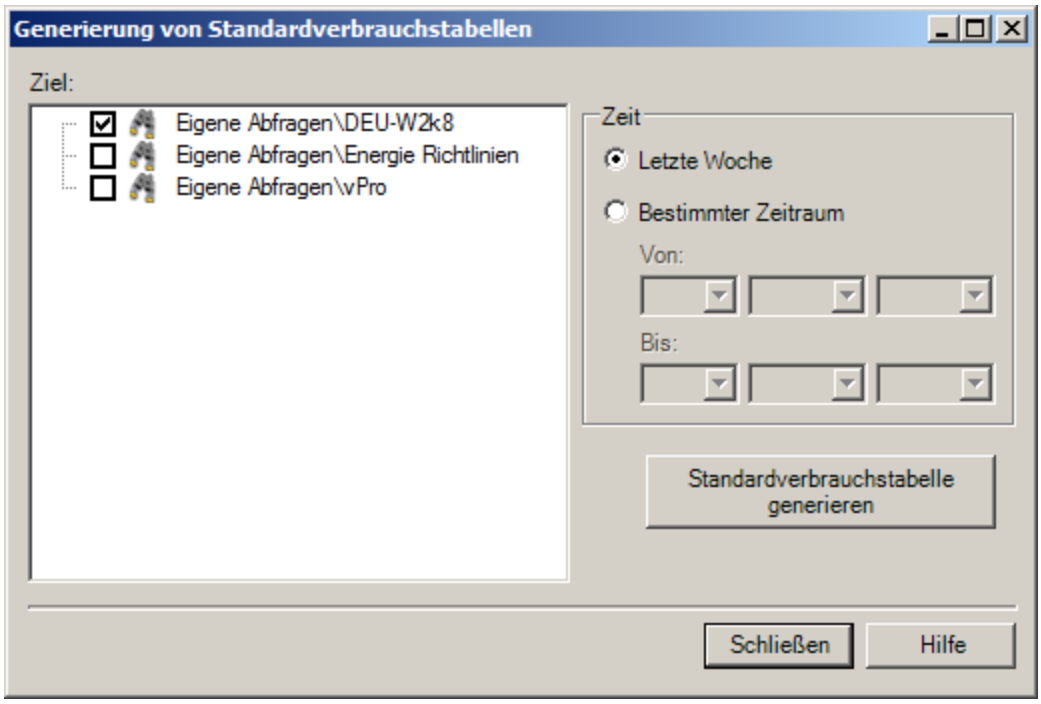
1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anpassen** ( ) und wählen Sie **Benutzerdef. Stromverbrauchseinstellungen** aus.
3. Deaktivieren Sie das Kontrollkästchen **Standardeinstellungen**.
4. Geben Sie den Namen des **Herstellers** und den Namen bzw. die Nummer des **Modells** für den Gerätetyp ein, den Sie verwenden möchten.
5. Wählen Sie den Gehäusetyp aus, der dem Gerät entspricht.

6. Fügen Sie die Stromverbrauchsdaten für den Computer und den Monitor in den verschiedenen Energiezuständen hinzu.
7. Klicken Sie auf **Schließen**, um die Daten für dieses Modell zu speichern.

Generieren einer XML-Datei für die Standardverbrauchstabelle

Berichte zur Energieverwaltung verwenden Durchschnittsdaten für verschiedene Typen von Computern (Desktop-, Notebook- oder Laptop-Computer). Wenn Sie einen Bericht für eine Gruppe von Computern generieren, werden die Computer in dieser Gruppe mit den durchschnittlichen Stromverbrauchsdaten der entsprechenden Computertypen abgeglichen. Die Daten basieren demnach auf einem Durchschnittsverbrauch und nicht auf dem spezifischen Stromverbrauch.

Diese durchschnittlichen Daten sind in einer XML-Daten enthalten. Wenn Sie Vergangenheitsdaten von Ihren verwalteten Geräten gesammelt haben, können Sie eine neue XML-Datei generieren, die anstelle der Durchschnittsdaten Daten von Ihren eigenen verwalteten Geräten verwendet. Diese XML-Datei tritt an die Stelle der Standarddatei. Sie gibt den Stromverbrauch in Ihrem Unternehmen wieder und liefert so einen präziseren Bericht zu den Einsparungen.



So generieren Sie eine XML-Datei für die Standardverbrauchstabelle

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Anpassen** ( ) und wählen Sie **Angenommenen Clientverbrauch durch Vergangenheitsdaten ersetzen**.
3. Wählen Sie Gerätegruppen oder Abfragen aus, die Sie zur Berechnung der Daten verwenden möchten.
4. Wählen Sie den Zeitraum aus, für den Sie neue Daten berechnen möchten. Sie können die neueste

Woche wählen oder einen bestimmten Zeitraum angeben.

5. Klicken Sie auf **Standardverbrauchstabelle generieren**.

Eine neue XML-Datei wird erstellt. Die Daten in dieser Datei werden für die Berechnungen zur Erstellung von Einsparungsberichten verwendet.

HINWEIS: Damit Sie eine neue XML-Datei generieren können, müssen Sie Vergangenheitsdaten von verwalteten Geräten für eine Zeitraum besitzen, der mindestens der in diesem Dialogfeld ausgewählten Zeitspanne entspricht. Liegen nicht genügend Vergangenheitsdaten vor, können Sie keine neue XML-Datei generieren.

Anzeigen des Alarmprotokolls zur Energieverwaltung

Bei der Ausführung von Energieverwaltungsrichtlinien auf verwalteten Geräten können Situationen auftreten, in denen Geräte nicht wie erwartet auf Energiesparaktionen reagieren. Ein Prozess, der auf einem Gerät ausgeführt wird, bleibt unter Umständen weiter aktiv, selbst wenn ein Befehl zum Wechsel des Energiezustands an das Gerät gesendet wird.

Im Alarmprotokoll werden Einzelheiten zu solchen Konflikten aufgelistet. Sie können die Informationen in diesem Protokoll zur Verwaltung von Anwendungen auf Geräten verwenden und angeben, welche Anwendungen weiter ausgeführt werden dürfen oder beendet werden sollen, wenn ein Energiesparvorgang geplant ist.

So zeigen Sie das Alarmprotokoll zur Energieverwaltung an

1. Klicken Sie auf **Extras > Energieverwaltung > Energieverwaltung**.
2. Klicken Sie in der Strukturansicht auf dem Knoten **Alarmprotokoll**.
3. Um Alarme zu einem bestimmten Gerät oder für einen bestimmten Datumsbereich zu finden, geben Sie eine Suchzeichenfolge in das Feld **Suchen** ein, wählen Sie eine Spalte oder einen Datumsbereich aus und klicken Sie dann auf die Schaltfläche **Suchen**.

Wenn Sie Prozesse identifiziert haben, die Konflikte auslösen, verwenden Sie die Symbolleistenoptionen für die Anwendungsverwaltung, um die Art und Weise zu ändern, wie eine Energierichtlinie ausgeführt wird, wenn bestimmte Anwendungen auf einem Gerät ausgeführt werden. Weitere Informationen finden Sie unter "Verwalten von Anwendungen, die mit Energierichtlinien in Konflikt stehen" auf Seite 821.

Alarmfunktion

Alarme und Überwachung – Übersicht

Durch die LANDesk Management Suite Alarmierungs- und Überwachungsfunktionen werden Sie unmittelbar von Hardware-, Software- und Anwendungsereignissen auf Ihren verwalteten Geräten in Kenntnis gesetzt. Wenn Ereignisse auftreten, die Ihr Eingreifen erforderlich machen oder auf ein potentielles Problem hinweisen, leiten Alarme die Problemlösung durch Protokollieren des Ereignisses, durch Senden einer E-Mail oder Pager-Meldung, Ausführen einer Anwendung oder Abschalten des Geräts ein.

Die folgenden allgemeinen Arten der Überwachung stehen in Management Suite zur Verfügung.

- Überwachen (Pingen) von Geräten auf Netzwerkkonnektivität
- Grundlegende Hardware- und Softwareüberwachung für alle Geräte
- Leistungsüberwachung für ausgewählte Hardwarefunktionen
- Hardwareabhängige Überwachung unter Einsatz der Überwachungstechnologie des Herstellers

Management Suite bietet eine integrierte Alarmierung für diese Arten der Überwachung. Die Alarme, die Sie zur Anwendung auf bestimmte Geräte auswählen, sind in Alarmregelsätzen enthalten, die Sie verteilen.

Alle Alarme und die Überwachung sind von der Art der Hardware, der Firmware und den damit im Zusammenhang stehenden Funktionen und Merkmalen des jeweiligen Geräts abhängig. Manche Überwachungsoptionen werden nur auf bestimmten Gerätetypen unterstützt. In manchen Fällen kann die Implementierung eines Hardwarestandards von Hersteller zu Hersteller variieren, d. h. was auf einem Gerät funktioniert, kann unter Umständen so auf einem anderen Gerät nicht funktionieren.

Grundlegendes zu Alarmen, Regeln und Regelsätzen

Ein *Alarm* ist eine eindeutige Kennung, die ein Ereignis darstellt. Sie können eine *Alarmaktion* angeben, die automatisch durchgeführt wird, wenn das Ereignis auftritt, z. B. eine automatisierte E-Mail, Anwendungen oder Stromoptionen.

Ein Alarm, der mit einer Aktion kombiniert ist, wird in diesem Produkt als eine *Alarmregel* bezeichnet. Manche Alarme können mit bestimmten *Leistungsüberwachungsregeln* kombiniert werden, die den Zustand angeben, der ein Ereignis auslöst. Sie können beispielsweise eine Überwachungsregel für den verfügbaren, freien Festplattenspeicher definieren, damit ein Alarm ausgelöst wird, wenn das Laufwerk zu 90 Prozent ausgelastet ist.

Bei der Definition der *Alarmregelsätze* entscheiden Sie, welche Ereignisse sofortige Maßnahmen erfordern bzw. welche Ereignisse für Ihre Kenntnisnahme protokolliert werden sollen. Ein Regelsatz enthält diverse Alarmregeln, von denen jeder eine entsprechende Alarmaktion zugewiesen ist. Sie können Alarmregelsätze auf einem oder mehreren Geräten bereitstellen, um die Elemente zu überwachen, die für diese Art von Gerät wichtig sind.

Alarmagenten und Alarmregelsätze

Um Alarme für ein verwaltetes Gerät auszulösen, muss der LANDesk Alarmagent auf dem Gerät bereitgestellt sein. Ein Standardalarmagent und ein Standard-Alarmregelsatz werden für jedes verwaltete Gerät bei der Installation des Standardagenten auf dem Gerät bereitgestellt. Dieser Agent befolgt die Regeln, die in den Alarmregelsätzen für dieses Gerät definiert sind.

Standardmäßig hat jedes verwaltete Gerät einen Standardalarmregelsatz. Wenn Sie einen benutzerdefinierten Regelsatz bestimmt haben, können Sie ihn auf Geräten zur Überwachung von Elementen bereitstellen, die für diesen Gerätetyp üblich sind. Sie können mehrere Regelsätze auf den Geräten bereitstellen, obwohl Sie sich darüber bewusst sein sollten, dass zwischen ähnlichen Regeln in verschiedenen Regelsätzen Konflikte auftreten können.

HINWEIS: Wenn Sie eine zusätzliche Win32-Konsole auf einem Gerät installieren, wird auf diesem Gerät kein Agent installiert. Auch wenn Sie andere Geräte von dieser Konsole aus verwalten, kann das Konsolengerät selbst keine Alarme generieren, weder als Core noch als verwaltetes Gerät, außer Sie installieren außerdem noch Managementagenten darauf.

Grundlegendes zur Leistungsüberwachung

Manche Alarmereignisse basieren auf bestimmten Leistungsüberwachungsregeln. *Leistungsüberwachung* bezieht sich auf ein Ereignis auf der Basis von Leistungszählern, die für bestimmte Geräte definiert wurden. Zähler können für Hardwarekomponenten und -sensoren, Betriebssystemleistung, Anwendungskomponenten und Nutzungsniveaus definiert werden.

Um einem Regelsatz für ein Gerät die Leistungsüberwachung hinzuzufügen, wählen Sie die Leistungsüberwachungsalarmregel im Regelsatz aus. Was genau überwacht werden soll wird jedoch für jedes einzelne Gerät festgelegt. Dies erfolgt in der Konsole für Echtzeitinventar- und -überwachung auf jedem Gerät. Sie können verschiedene Hardware- und Softwarekomponenten auswählen und die Zähler für die Elemente definieren, die gepollt werden sollen, und dann die Überwachungsdaten in Echtzeit oder im Verlauf anzeigen.

Hardwarespezifische Überwachung

Management Suite bietet Unterstützung für die folgenden Überwachungstechnologien für die Hardware verschiedener Hersteller:

- IPMI (Intelligent Platform Management Interface) 1.5 und 2.0
- IPMI BMC (Baseboard Management Controller)-Konfiguration
- Dell OMCI (OpenManage Client Instrumentation)
- Dell DRAC (Dell Remote Access Controller)
- Intel vPro-Technologie, einschließlich Intel AMT (Active Management Technology)

Echtzeitinventar und Überwachung – Übersicht

LANDesk Management Suite bietet über die Konsole "Echtzeitinventar und Überwachung" Echtzeit-Updates für Inventardaten und den Überwachungsstatus.

Diese Konsole steht nur für Geräte zur Verfügung, bei denen im LANDesk Agenten die Optionen für Echtzeitinventar und Überwachung aktiviert wurden.

Öffnen der Konsole

Sie können die Konsole "Echtzeitinventar und Überwachung" auf zweierlei Weise öffnen:

- Klicken Sie mit der rechten Maustaste in der Netzwerkansicht auf ein verwaltetes Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus. Diese Option steht nicht zur Verfügung, wenn bei dem Gerät die Überwachungsoption im LANDesk Agenten nicht aktiviert wurde.

- Öffnen Sie das Health-Dashboard. (Klicken Sie auf **Extras > Berichte/Überwachung > Health Dashboard**.) Klicken Sie mit der rechten Maustaste auf ein Gerät und wählen Sie **Details anzeigen** aus. Die Konsole "Echtzeitinventar und Überwachung" wird für alle Geräte geöffnet, Echtzeitdaten stehen aber nur dann zur Verfügung. wenn bei einem Gerät im LANDesk Agenten die Überwachungsoption aktiviert wurde.

Überwachen von Geräten auf Netzwerkkonnektivität

Mithilfe der Geräteüberwachung können Sie regelmäßig die Konnektivität der verwalteten Geräte überwachen.

Die Pingeinstellungen gelten speziell für das Gerät, das Sie ausgewählt haben. Wenn ein Gerät nicht mehr auf einen Ping reagiert (also offline ist) wird eine Alarmbenachrichtigung zum Protokoll auf dem Coreserver hinzugefügt. Wenn Sie durch eine andere Alarmaktion benachrichtigt werden wollen, beispielsweise indem Sie eine E-Mail erhalten, wenn ein Gerät offline geht, können Sie einen Alarm im Alarmregelsatz des Cores konfigurieren.

So überwachen Sie die Konnektivität von verwalteten Geräte

1. Klicken Sie auf **Konfigurieren > Geräteüberwachung**.
2. Klicken Sie auf **Hinzufügen**. Wählen Sie ein oder mehrere Geräte aus, die Sie überwachen möchten und klicken Sie dann auf **Hinzufügen**.
3. Definieren Sie die Einstellung der **Pingfrequenz**, die Anzahl der Wiederholungen und das Timeoutlimit.
4. Klicken Sie auf **OK**.

Klicken Sie hier, um Details zum Dialogfeld "Geräteüberwachung konfigurieren" abzurufen.

In diesem Dialogfeld können Sie folgende Optionen für die Geräteüberwachung konfigurieren:

- **Diese Geräte überwachen:** Gibt die derzeit überwachten Geräte an.
- **Hinzufügen:** Öffnet das Dialogfeld **Überwachte Geräte hinzufügen**. Dort können Sie nach verwalteten Geräten suchen und verwaltete Geräte aussuchen, die Sie überwachen möchten.
- **Entfernen:** Entfernt das ausgewählte Gerät aus der Liste.
- **Pingfrequenz:** Steuert, wann und wie der Pingvorgang abläuft. Diese Einstellungen können auf jedes Gerät einzeln übertragen werden.
    - **Ping alle:** Plant einen regelmäßigen Ping im festgelegten Minutenintervall.
    - **Täglich planen um:** Plant einen täglichen Ping zu einer festgelegten Zeit.
    - **Versuche:** Legt die Anzahl der Pingwiederholungen fest.
    - **Timeout:** Legt die Anzahl der Sekunden fest, bis das Timeout für die Pingwiederholungen eintritt.

Konfigurieren von Geräteüberwachungsalarmen

Damit Sie von der Geräteüberwachung benachrichtigt werden, wenn verwaltete Geräte online oder offline gehen, müssen Sie zuerst einen Alarmregelsatz mit zusätzlichen Aktionen konfigurieren (wie z. B. Empfang einer E-Mail, wenn ein Alarm gesendet wird).

So konfigurieren Sie Alarmeinstellungen für die Geräteüberwachung

1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Erweitern Sie im Baum **Alarme** das Element **Alarmregelsätze**.
3. Klicken Sie mit der rechten Maustaste auf **Core-Alarmregelsätze** und klicken Sie dann auf **Bearbeiten**.
4. Klicken Sie im Fenster **Regelsatz** im Bereich **Alarmregelsatz** auf **Alarme**.
5. Klicken Sie im Bereich **Alarme** unter dem Order **Standard** auf **Geräteüberwachung**.
6. Klicken Sie im rechten Fensterausschnitt auf **Regeln > Hinzufügen**.
7. Ziehen Sie den Alarm **Geräteüberwachung – Systemkonnektivität** auf den Auswahlbereich **Alarme** am unteren Rand der Seite.
8. Klicken Sie im Fenster **Regelsatz** im Bereich **Alarmregelsatz** links auf **Aktionen** und ziehen Sie beliebige zusätzliche Regelsätze nach unten auf den Auswahlbereich **Aktionen**. Die Core-Alarmprotokoll-Handlerkonfiguration bildet die standardmäßige Aktion. Sie können entscheiden, ob Sie beim Empfang eines Alarms eine E-Mail oder einen SNMP-Trap senden oder eine ausführbare Datei auf dem Core ausführen möchten. (Unter Umständen müssen Sie jede Aktion definieren, z. B. angeben, wohin die E-Mail-Alarme gesendet werden sollen.)
9. Klicken Sie im Fenster **Regelsatz** links im Bereich **Alarmregelsatz** auf **Zeit** und ziehen Sie **Immer** nach unten auf den Auswahlbereich **Zeit**.
10. Klicken Sie neben den Auswahlbereichen auf die Schaltfläche **OK**.
11. Klicken Sie im rechten Fensterausschnitt **Aktionen** auf **Veröffentlichen**.
12. Klicken Sie im linken Fensterbereich **Alarmregelsatz** auf **Regelübersicht** und doppelklicken Sie dann auf die von Ihnen erstellte Regel.
13. In dem daraufhin angezeigten Dialogfeld markieren Sie das Kontrollkästchen **Zustand**, wenn sich der Gerätezustand in der Konsole ändern soll, je nachdem, ob das Gerät online oder offline ist. Klicken Sie dann auf **OK**.
14. Klicken Sie auf **Veröffentlichen**, um alle Änderungen zu veröffentlichen, die Sie vorgenommen haben und das Fenster **Regelsatz** zu schließen.

HINWEIS: Wenn Sie Alarmeinstellungen konfigurieren, werden diese auf alle von Ihnen überwachten Geräte angewendet.

Deaktivieren des ModemView-Dienstes

Der ModemView-Dienst ist der Dienst/Treiber, der Modemanrufe (sowohl ankommende als auch ausgehende) überwacht und einen Alarm generiert, wenn ein Anruf registriert wird. Dieser Dienst beansprucht 10 MB, da er mit MFC arbeitet. Es ist für Sie unter Umständen nicht sinnvoll, diesen Dienst auszuführen, insbesondere, wenn kein Modem an das Gerät angeschlossen ist.

So deaktivieren Sie den ModemView-Dienst

1. Klicken Sie auf dem Gerät (entweder direkt oder remote) auf **Start > Systemsteuerung > Verwaltung > Dienste**.
2. Doppelklicken Sie auf **LANDesk Message Handler Service**.
3. Wählen Sie unter **Starttyp** die Einstellung **Manuell** aus und klicken Sie auf **OK**.

Sie können auch auf **Beenden** unter **Dienststatus** klicken.

Grundlagen der Alarmierung

Um Alarme für ein verwaltetes Gerät auszulösen, muss der Management Suite Alarmagent auf dem Gerät bereitgestellt sein. Ein Standardalarmagent und ein Standard-Alarmregelsatz werden für jedes verwaltete Gerät bereitgestellt, wenn der Standardagent auf dem Gerät installiert wird. Dieser Agent befolgt die Regeln, die in den Alarmregelsätzen für dieses Gerät definiert sind.

Wenn Sie einen benutzerdefinierten Regelsatz bestimmt haben, können Sie ihn auf Geräten zur Überwachung von Elementen bereitstellen, die für diesen Gerätetyp üblich sind. Sie können mehrere Regelsätze auf den Geräten bereitstellen, obwohl Sie sich darüber bewusst sein sollten, dass zwischen ähnlichen Regeln in verschiedenen Regelsätzen Konflikte auftreten können.

Ereignisse, die Alarme auslösen können

Dieses Produkt verfügt über eine umfassende Liste mit Ereignissen, die Alarme auslösen können. Manche Ereignisse sind Probleme, die Ihre unmittelbare Aufmerksamkeit erfordern, z. B. ein Komponentenfehler oder Systemausfall. Andere Ereignisse sind Konfigurationsänderungen, die einem Systemadministrator nützliche Informationen geben, wie beispielsweise Änderungen, die die Leistung und Stabilität eines Geräts beeinflussen oder Probleme bei einer Standardinstallation verursachen.

Beispiele für die Ereignistypen, die Sie überwachen können, sind unter anderem:

- **Hardwareänderungen:** Eine Komponente, beispielsweise ein Prozessor, ein Speichermodul, ein Laufwerk oder eine Karte, wurden hinzugefügt oder entfernt.
- **Hinzugefügte oder entfernte Anwendung:** Ein Benutzer hat eine Anwendung auf einem Gerät installiert oder deinstalliert. Diese Informationen können sich für die Überwachung der Lizenznutzung oder Mitarbeiterproduktivität als nützlich erweisen. Anwendungen, die in Windows "Programme hinzufügen oder entfernen" registriert sind, werden überwacht und der Name der Anwendung, der in "Programme hinzufügen oder entfernen" verwendet wird, ist der Name, der in der Alarmbenachrichtigung erscheint.
- **Dienstereignis:** Auf dem Gerät wurde ein Dienst gestartet oder gestoppt.
- **Leistung:** Ein Leistungsgrenzwert wurde überschritten, beispielsweise die Laufwerkskapazität, verfügbarer Speicherplatz und so weiter.
- **IPMI-Ereignis:** Ein Ereignis, das auf IPMI-Geräten registriert werden kann, ist aufgetreten – beispielsweise Änderungen an den Controllern, Sensoren, Protokollen und so weiter.
- **Modemverwendung:** Das Systemmodem wurde benutzt, oder ein Modem wurde hinzugefügt oder entfernt.
- **Physikalische Sicherheit:** Erkennung eines unbefugten Gehäusezugriffs, eines Energiezyklus (Ein-/Ausschalten) oder einer anderen physikalischen Änderung.
- **Paketinstallation**: Auf dem Zielcomputer wurde ein Paket installiert.
- **Remotesteuerungsaktivität:** Aktivität im Zusammenhang mit einer Remotesteuerungssitzung wurde registriert, einschließlich Start, Stopp oder Fehler.

Um einen Datensatz mit Alarmmeldungen anzuzeigen, die aus Konfigurationsänderungen resultieren, überprüfen Sie das Alarmprotokoll in der Echtzeitinventar- und Überwachungskonsole des Geräts.

Alarme können nur generiert werden, wenn Geräte mit der entsprechenden Hardware ausgerüstet sind. Von einem Sensor generierte Alarme sind nur für Geräte relevant, die mit den korrekten Sensoren ausgestattet sind.

Die Hardwareüberwachung hängt außerdem von der korrekten Konfiguration der Hardware ab. Wenn z. B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden durch die S.M.A.R.T.-Laufwerksüberwachung keine Alarme generiert.

Schweregrade von Ereignissen

Geräteprobleme oder Ereignisse können mit einigen oder allen der nachstehend genannten Schweregraden verknüpft werden. In manchen Teilen der Produktschnittstelle werden diese Zustände mit einem Zahlenwert und einem dazugehörigen Symbol vermerkt. Die Zahlenwerte sind in Klammern dargestellt.

- **Zu Informationszwecken (1)**: Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen. Dieser Schweregrad wirkt sich nicht auf den Gerätezustand aus.
- **OK (2):** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.
- **Warnung (3)**: Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
- **Kritisch (4)**: Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Unbekannt:** Der Alarmstatus lässt sich nicht bestimmen oder der Überwachungsagent ist nicht auf dem Gerät installiert.

Je nachdem, um welches Ereignis es sich handelt, sind einige Schweregrade nicht relevant und deshalb nicht verfügbar. Beispiel: Bei einem Intrusion Detection-Ereignis ist das Gehäuse des Geräts entweder offen oder geschlossen. Ist es offen, kann eine Alarmaktion ausgelöst werden, aber nur beim Schweregrad "Warnung". Andere Ereignisse, z. B. Speicherplatz und virtueller Speicher enthalten drei Schweregrade (OK, Warnung und kritisch), weil verschiedene Zustände den Administrator auf verschiedene Besorgnisstufen aufmerksam machen.

Sie können den Schweregrad oder Grenzwert auswählen, der bestimmte Alarme auslösen wird. Sie können beispielsweise eine Aktion für einen Warnstatus eines Alarms auswählen und eine andere Aktion für einen kritischen Status. Der Status "Unbekannt" kann nicht als Alarmauslöser ausgewählt werden; er gibt lediglich an, dass sich der Status nicht bestimmen lässt.

Alarmaktionen für Benachrichtigungen

Dieses Produkt kann Sie folgendermaßen benachrichtigen, wenn ein überwachtes Ereignis eintritt:

- Hinzufügen von Informationen zum Protokoll
- Benachrichtigung per E-Mail oder Übermittlung einer Pager-Nachricht
- Ausführen eines Programms auf dem Core oder auf einem bestimmten Gerät
- Weiterleiten einer SNMP-Trap an eine SNMP-Verwaltungskonsole im Netzwerk
- Neustarten oder Herunterfahren eines Geräts

Alarmaktionen werden beim Definieren der Alarmregelsätze konfiguriert.

Alarmsturmsteuerung

Manche den Gerätegruppen zugeordneten Alarmregeln können simultan sehr viele Reaktionen generieren. Beispiel: Sie konfigurieren eine Alarmregel für Änderungen an der Computerkonfiguration und verknüpfen sie mit einer E-Mail-Aktion. Wenn ein Softwareverteilungspatch auf viele Computer übertragen wird, auf denen diese Alarmeinstellung aktiviert wurde, würden durch dieses Patch auf dem Coreserver so viele E-Mails generiert wie Geräte vorhanden sind, auf die das Patch übertragen wurde; d. h., auf Ihren E-Mail-Server käme möglicherweise ein Ansturm von E-Mails zu.

Die Alarmsturmsteuerung dieses Produkts beschränkt die Häufigkeit, mit der eine Alarmaktion für einen Alarm ausgeführt wird, automatisch. Wenn ein Alarm eine Aktion 5-mal in 5 Minuten auslöst, dann wird zwar die Alarmaktion abgebrochen, der Alarm wird jedoch trotzdem in die Coreprotokolldatei geschrieben. Der Administrator wird von dem Alarmsturm über eine automatische E-Mail benachrichtigt. Wenn ein Alarm nicht mehr auftritt und mindestens eine Stunde lang inaktiv war, wird die Alarmsturmsteuerung für diesen Alarm zurückgesetzt. Die Alarmaktionen werden dann wieder ausgelöst, wenn der Alarm später erneut auftritt.

Bereitstellung von Alarmregelsätzen

Dieses Produkt enthält vordefinierte Alarmregelsätze, die auf verwalteten Geräten bereitgestellt werden können. Beachten Sie, dass auf jedem verwalteten Gerät ein Managementagent installiert sein muss, bevor Sie einen Alarmregelsatz auf dem Gerät bereitstellen können und bevor es Alarmmeldungen an den Coreserver senden kann.

Standardregelsätze

Beim Installieren des Überwachungsagenten auf einem verwalteten Gerät wird der **LDMS-Standardregelsatz** installiert, um Feedback-Meldungen bezüglich des Systemzustands an das Health Dashboard und die Konsole weiterzuleiten. Dieser Standardregelsatz schließt unter anderem folgende Alarme ein:

- Datenträger hinzugefügt oder entfernt
- Laufwerksspeicher
- Speichernutzung
- Temperatur, Lüfter und Spannung
- Remotesteuerungsaktivitäten
- Leistungsüberwachung
- IPMI-Ereignisse (auf relevanter Hardware)
- Inventarscanneralarme
- Aktionen des Connection Control Managers
- LANDesk Antiviruszustand
- Zustand der Netzwerkzugriffskontrolle
- Client-Datenbankprogramm
- Sicherheits- und Patchmanagement-Alarme

Sie können den LDMS-Standardregelsatz ändern, um die gewünschten Alarme zur Überwachung einzufügen.

Benutzerdefinierte Alarmregelsätze

Zusätzlich zu diesen Standardregelsätzen können Sie benutzerdefinierte Alarmregelsätze konfigurieren und bereitstellen. Sie können in diese Gruppen benutzerdefinierte Alarmaktionen einschließen, um auf jede beliebige Kombination von Ereignissen zu reagieren. Sie können z. B. einen Aktionssatz definieren für Ereignisse auf verwalteten Desktopgeräten (z. B. eine E-Mail ans Hardware-Support-Team senden) und einen anderen Aktionssatz für verwaltete Server (z. B. eine Pagermeldung an Admin senden).

Prozess für die Bereitstellung von Regelsätzen

Der allgemeine Prozess für das Bereitstellen von Alarmregelsätzen auf verwalteten Geräten sieht wie folgt aus:

1. Erstellen oder bearbeiten Sie den Regelsatz.
2. Erstellen Sie einen Task zur Planung der Bereitstellung des Regelsatzes.
3. Wählen Sie die Geräte aus, für die der Regelsatz bereitgestellt werden soll und führen Sie den Planungstask aus.
4. Wenn ein Regelsatz Leistungsüberwachungsalarme umfasst, öffnen Sie die Konsole "Echtzeitinventar und Überwachung" für jedes Gerät mit diesem Regelsatz und definieren Sie die Leistungsüberwachungszähler für das Gerät.

Verwandte Themen

"Konfigurieren von Alarmregelsätzen" auf Seite 842

"Bereitstellen eines Alarmregelsatzes" auf Seite 839

"Informationen zur Leistungsüberwachung" auf Seite 855

"Verwenden von Agentenkonfigurationen" auf Seite 107

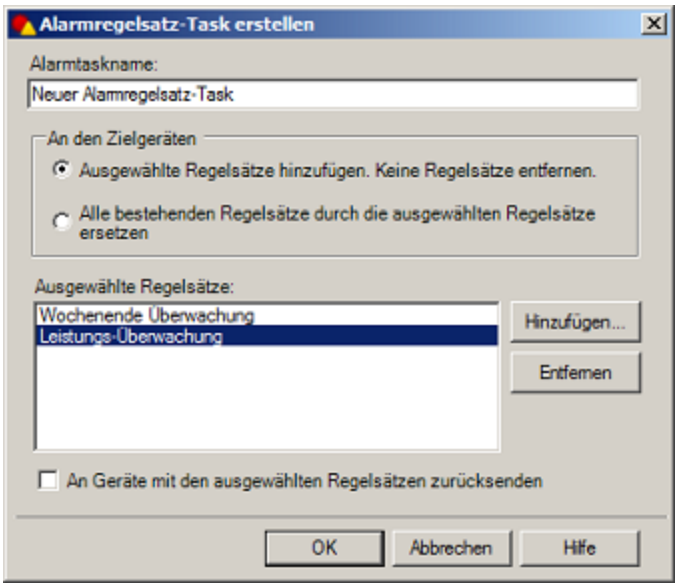
Bereitstellen eines Alarmregelsatzes

Um einen Alarmregelsatz auf einem oder mehreren Geräten zu installieren, können Sie einen Bereitstellungstask für den Regelsatz planen.

Bevor Sie einen Regelsatz auf einem verwalteten Gerät bereitstellen, muss zuvor auf diesem Gerät ein Management-Agent installiert werden. Wenn Sie den Standard-Managementagenten bereitstellen, wird der Standardregelsatz auf dem Gerät standardmäßig installiert, aber sie können wählen, ob dieser oder irgendein anderer verfügbarer Regelsatz auf dem Gerät mit dem Managementagenten installiert werden soll. Nachdem das Agenten-Setup vollständig ausgeführt wurde, können Sie den Standardregelsatz aktualisieren oder neue Regelsätze bereitstellen, indem Sie einen Alarmtask planen.

So stellen Sie einen Alarmregelsatz bereit

1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Wählen Sie in der Liste **Alarmregelsätze** den Regelsatz aus, den Sie bereitstellen möchten.
3. Klicken Sie in der Symbolleiste auf das Symbol **Task erstellen** und wählen Sie **Regelsätze verteilen**.



4. Geben Sie einen Tasknamen für den Alarmtask ein.
5. Um den Regelsatz zu Geräten hinzuzufügen und alle auf diesen Geräten vorhandenen Regelsätze beizubehalten, klicken Sie auf **Ausgewählte Regelsätze hinzufügen.**

   Um den Regelsatz zu Geräten hinzuzufügen und alle auf diesen Geräten vorhandenen Regelsätze zu löschen, klicken Sie auf **Alle bestehenden Regelsätze durch die ausgewählten Regelsätze ersetzen**.

   Wenn Sie zuvor bereits einen Regelsatz bereitgestellt haben und ihn auf denselben Geräten aktualisieren möchten, dann markieren Sie das Kästchen **An Geräte mit den ausgewählten Regelsätzen zurücksenden**.
6. Um andere Regelsätze auf demselben Task bereitzustellen, klicken Sie auf die Schaltfläche **Hinzufügen** und wählen die Regelsätze aus.
7. Klicken Sie auf **OK**.

   Im Extra **Geplante Tasks** wird ein neuer Task erstellt.

8. Ziehen Sie Geräte von der Netzwerkansicht auf den neuen Alarmtask.
9. Klicken Sie mit der rechten Maustaste auf den Task und wählen Sie **Eigenschaften** aus. Vergewissern Sie sich, dass Sie die korrekten Zielgeräte haben und wählen Sie dann die gewünschten Optionen zur Planung des Tasks aus und klicken Sie anschließend auf **Speichern**.

Hinweise

- Sie können die Regelsätze als Teil der Agentenkonfiguration auf den Geräten bereitstellen. Wenn Sie eine Agentenkonfiguration definieren, können Sie die Regelsätze auswählen, die Sie bereitstellen möchten.

- Wenn der bereitgestellte Regelsatz eine Leistungsüberwachungsregel enthält, werden die Details der Überwachung auf jedem einzelnen Gerät definiert. Dies erfolgt in der Konsole für Echtzeitinventar- und -überwachung auf jedem Gerät. Sie können verschiedene Hardware- und Softwarekomponenten auswählen und die Zähler für die Elemente definieren, die gepollt werden sollen, und dann die Überwachungsdaten in Echtzeit oder im Verlauf anzeigen.

Verwandte Themen

"Erstellen einer Agentenkonfiguration" auf Seite 108

"Informationen zur Leistungsüberwachung" auf Seite 855

Anzeigen von Alarmregelsätzen für ein Gerät

Um die Alarmregelsätze anzuzeigen, die den verwalteten Geräten hinzugefügt wurden, öffnen Sie die vollständige Inventaransicht für das Gerät. Hier wird der Name des Regelsatzes und das Datum seiner letzten Installation oder Aktualisierung auf den Gerät angezeigt.

So zeigen Sie die auf einem Gerät installierten Alarmregelsätze an

1. Rechtsklicken Sie in der Ansicht **Alle Geräte** auf das Gerät und wählen Sie **Inventar**.
2. Erweitern Sie **LANDesk Management** in der Strukturansicht und klicken Sie auf **Installierter Alarmregelsatz**.
3. Wenn es mehr als einen Regelsatz gibt, wählen Sie einen Regelsatz in der Strukturansicht aus, um seine Einzelheiten anzuzeigen.

HINWEIS: Sie können eine Abfrage erstellen, die alle Geräte zurückgibt, auf denen ein bestimmter Alarmregelsatz installiert ist. Folgen Sie in der Abfragekomponentenliste demselben Pfad, der in der o.g. Inventarliste beschrieben ist.

Entfernen aller Regelsätze von einem Gerät

Sie können alle Regelsätze von einem oder mehreren Geräten entfernen, ohne dass Sie irgendwelche neuen Regelsätze bereitstellen.

Sie können alle Regelsätze entfernen, wenn auf einem Gerät ein oder mehrere Regelsätze gelten und Sie diese durch einen neuen Regelsatz ersetzen wollen. Wenn auf einem Gerät mehrere Regelsätze Gültigkeit haben, kann dies zu unvorhergesehenen Ergebnissen führen, da ähnliche Alarmregelsätze unter Umständen widerstreitende Aktionen aufweisen und unbeabsichtigte Resultate nach sich ziehen können.

So entfernen Sie alle vorhandenen Regelsätze

1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Klicken Sie in der Symbolleiste auf das Symbol **Task erstellen** und wählen Sie **Alle Regelsätze entfernen**.
3. Klicken Sie auf **OK**.

Migrieren von Alarmen aus früheren Versionen

Vorige Versionen von LANDesk Management Suite beinhalteten die Alarmfunktionalität in der Funktion "Alarm-Management-System" (AMS). Ab Version 8.8 basiert die Alarmierung auf einem neuen Satz von Alarmhandlers, auch wenn manche Alarme auf AMS-Alarmmeldungen basieren. Sie müssen Ihren Alarmregelsatz für verwaltete Geräte mit der neuen Alarmfunktion erstellen.

Um Ihnen beim Migrieren von Alarmen aus älteren Versionen als 8.8 behilflich zu sein, ist in diesem Produkt ein Dienstprogramm enthalten, das Informationen über Ihre AMS-Alarme extrahiert und die Daten in eine Textdatei schreibt, auf die Sie zurückgreifen können, wenn Sie neue Regelsätze erstellen.

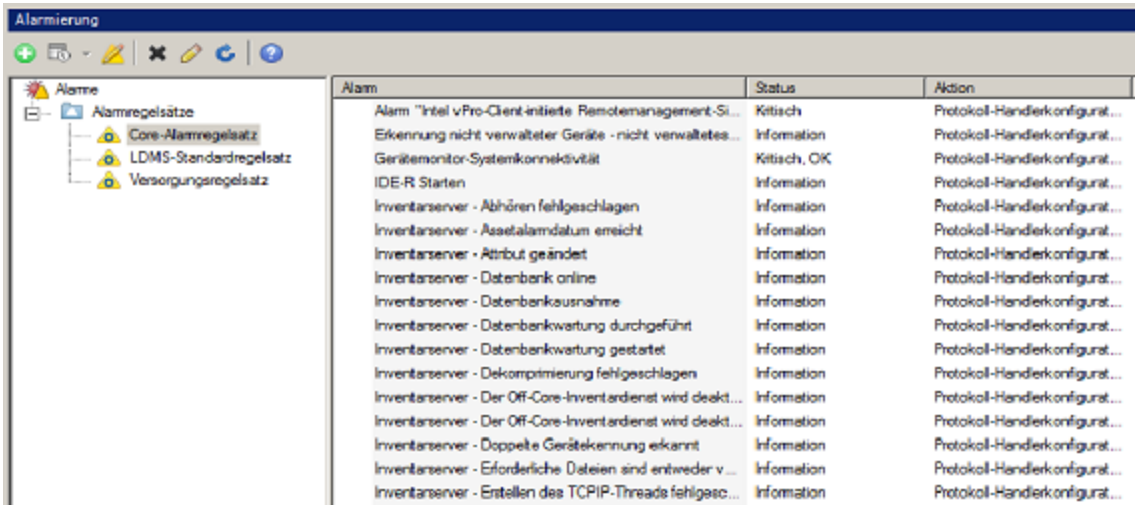
So verwenden Sie das Dienstprogramm für die Alarmmigration

1. Führen Sie im Verzeichnis \utilities der LDMAIN-Freigabe die Datei alertexp.exe aus.
   Zum Anzeigen von Hilfeinformationen zur Verwendung des Dienstprogramms geben Sie Folgendes in die Befehlszeile ein: `alertexp.exe /?`. Sie können auch wahlweise den Pfad zur iaobind.dat-Datei und einen Pfad und Dateinamen für die Ausgabedatei eingeben.
2. Öffnen Sie die Datei iaobind.txt, um eine Übersicht der bestehenden AMS-Alarme anzuzeigen.

Sie können die Information über Ihre bestehenden Alarme zum Erstellen neuer Alarmregelsätze verwenden. Die Textdatei führt den Namen aller Alarme und ihrer verknüpften Aktionen und Schweregrade sowie die Anwendung auf, die den Alarm auslöst und die damit verbundenen Parameter.

Konfigurieren von Alarmregelsätzen

Auf der Seite **Alarmregelsätze** finden Sie alle Alarmregelsätze, die Sie auf verwalteten Geräte bereitstellen können. Es gibt vier Standardregelsätze und Sie können benutzerdefinierte Regelsätze erstellen, um verschiedenen Geräten bestimmte Überwachungstypen zuzuordnen.



Die vier Alarmregelsätze, die standardmäßig auf der Seite **Alarmregelsätze** angezeigt werden:

- **Core-Alarmregelsatz**: Dieser Regelsatz sorgt dafür, dass Alarme, die vom Coreserver ausgehen, bearbeitet werden. Dieser Regelsatz wird auf dem Coreserver installiert, kann aber nicht auf anderen Geräten installiert werden und es darf nur einen Core-Alarmregelsatz geben. Sie können den Regelsatz bearbeiten, aber nicht mehr vom Coreserver löschen. Dieser Regelsatz enthält eine vordefinierte Gruppe mit Alarmen, einschließlich Alarme vom Typ "Geräteüberwachung", "Intel vPro Alarm" und "Serial Over LAN-Sitzung".
- **LDMS Standardregelsatz**: Dieser Regelsatz wird standardmäßig auf allen von der LANDesk Management Suite verwalten Geräten bereitgestellt. Er enthält Alarme für Sicherheitsfunktionen, die in der Management Suite enthalten sind, wie z. B. Alarme für Echtzeitinventar und Überwachung, Network Access Control-Alarme, Inventarscanner- und Sicherheits- und Patchmanagement-Alarme.

- **Versorgungsregelsatz**: Dieser Regelsatz enthält Alarme, die sich auf die Versorgungstasks beziehen, z. B. Anfang und Ende des Tasks, Abschnitt abgeschlossen und falsche Prebootumgebung für das Betriebssystem. Bei der Versorgung eines Geräts wird dieser Regelsatz verwendet, um Alarme bzgl. des Fortschritts des Versorgungstasks zu senden. Der Regelsatz ist im Versorgungsagenten enthalten und muss nicht manuell bereitgestellt werden. Sie können diesen Regelsatz bearbeiten, um die mit den Versorgungsalarmen verknüpften Maßnahmen zu ändern (z. B. via E-Mail benachrichtigt zu werden, wenn der Versorgungstask abgeschlossen ist).

Zusätzlich zu diesen Regelsätzen können Sie benutzerdefinierte Regelsätze erstellen und sie auf Gruppen mit verwalteten Geräten anwenden. Sie können Regelsätze bereitstellen, indem Sie einen Bereitstellungstask planen, oder Regelsätze einschließen, wenn Sie mithilfe der Agentenkonfiguration Agenten auf Geräten bereitstellen. Obwohl es Standardregelsätze gibt, die mit Agenten bereitgestellt werden können, können Sie bei der Definition der Agentenkonfiguration auch festlegen, die Regelsätze nicht bereitzustellen.

Konflikte zwischen Regelsätzen

Berücksichtigen Sie beim Erstellen eines benutzerdefinierten Regelsatzes für ein bestimmtes Gerät, dass sich überschneidende oder miteinander in Konflikt stehende Alarmregeln vorhanden sein können (falls bereits ein Standardregelsatz auf dem Gerät bereitgestellt wurde). Wenn Sie den Standardregelsatz beim Konfigurieren des verwalteten Geräts bereitstellen und dann einen benutzerdefinierten Regelsatz bereitstellen, werden beide Regelsätze auf dem Gerät ausgeführt.

Beispiel: Wenn beide Regelsätze Alarme für denselben Alarmtyp generieren, jedoch unterschiedliche Aktionen in die Wege leiten, müssen Sie damit rechnen, dass Alarmaktionen doppelt ausgeführt werden oder unvorhersehbare Folgen haben.

Standardprotokollaktion

Jedes Mal, wenn Sie eine Alarmregel erstellen, wird die Regel automatisch mit einer "Protokoll-Handlerkonfiguration"-Aktion erstellt. Dies geschieht, damit jeder Alarm stets beim Coreserver protokolliert wird.

Diese Standardregel muss immer im Regelsatz enthalten sein: Sie können sie nicht löschen, außer Sie löschen alle Regeln für diesen bestimmten Alarm. In anderen Worten, wenn Sie drei Regeln für einen Alarm haben, können Sie die Standardregel nicht löschen, außer Sie löschen alle drei Regeln. Aber die beiden anderen Regeln für diesen Alarm können Sie einzeln löschen.

Prozess für das Konfigurieren von Regelsätzen

Regelsätze enthalten eine Kombination aus zugehörigen Alarmen, Aktionen und Zeitfiltern. Bei der Konfiguration eines Regelsatzes definieren Sie mehrere Aktionstasks und Zeitfilter, die wiederverwendet werden können. Das allgemeine Verfahren zur Konfiguration eines Regelsatzes besteht aus den folgenden Schritten:

1. Einen Regelsatz erstellen
2. Dem Regelsatz neue Alarmregeln hinzufügen
3. Alarmaktionen definieren, die in den Regeln verwendet werden sollen
4. Zeitfilter definieren, die in den Alarmregeln verwendet werden sollen
5. Alarmregeln in einem Regelsatz bearbeiten
6. Regelsätze in andere Regelsätze einschließen
7. Einen Regelsatz veröffentlichen

Klicken Sie hier, um ein Beispiel für die Konfiguration eines Regelsatzes anzuzeigen.

Beispiel: Konfigurieren eines Regelsatzes für die Alarmierung bei Verknappung von Festspeicherressourcen

Das nachfolgend beschriebene Verfahren ist ein einfaches Beispiel für den ersten Schritt bei der Konfiguration eines benutzerdefinierten Regelsatzes. In diesem Beispiel wird eine einzelne Alarmregel zu einem Regelsatz hinzugefügt.

1. Klicken Sie in der Coreserverkonsole auf **Konfiguration > Alarmierung**.
2. Klicken Sie in der Symbolleiste auf **Neu**. Geben Sie einen Namen für den Regelsatz und eine Beschreibung ein (z. B. "Laufwerkspeicher 90% ausgelastet") und klicken Sie auf **OK**.
3. Klicken Sie in der Liste **Alarmregelsätze** auf den Namen des neuen Regelsatzes und dann in der Symbolleiste auf **Bearbeiten**.
4. Klicken Sie im Fenster **Regelsatzkonfiguration** auf **Alarme** in der linken Spalte.
   Es wird eine Strukturansicht der Alarme dargestellt, mit einem Raster mit Alarmen und ihren Beschreibungen. Sie können auf **Alle Alarme** klicken, um alle verfügbaren Alarme anzuzeigen oder auf eine Kategorie in der Strukturansicht für eine bestimmte Gruppe von Alarmen. Je nachdem, welche Auflösung Ihr Bildschirm hat, kann es sinnvoll sein, die Spaltengröße zu ändern, damit Sie die Elemente in der Liste lesen können.
5. Klicken Sie in der Strukturansicht unter der Gruppe **Überwachen** auf den Alarm **Laufwerkspeicherplatz**.
6. Wählen Sie aus dem Raster die **Standardmäßige Festplattennutzung** aus und klicken dann in der rechten Spalte auf **Bearbeiten**.
7. Sie können im Dialogfeld **Überwachung des Laufwerkspeicherplatzes** das **Abfrageintervall** auf die Häufigkeit einstellen, mit der die Laufwerkspeicherauslastung überwacht werden soll. Um die Grenzwerte zu ändern, bei denen ein Alarm ausgelöst wird, klicken Sie auf **Laufwerkspeicherplatz** und stellen Sie die Prozentsätze für die Warnung und kritische Alarme ein. (Es handelt sich hierbei um den ausgelasteten Anteil des gesamten Laufwerkspeichers.) Klicken Sie auf **OK**, um die Einstellungen zu speichern.
8. Klicken Sie auf der Seite **Alarme** in der rechten Spalte auf **Regeln > Hinzufügen**.
   Es werden drei Auswahlfelder am unteren Seitenrand dargestellt. Kombinieren Sie mithilfe dieser Felder die Elemente Alarm, Aktion und Uhrzeit, um eine Alarmregel zu erstellen.
9. Ziehen Sie den Alarm **Standardmäßige Festplattennutzung** auf das Feld **Alarme**.
10. Klicken Sie in der linken Spalte auf **Aktionen**. Klicken Sie auf den Ordner **Standard**. Ziehen Sie **Alarm in lokales Ereignisprotokoll protokollieren** auf das Auswahlfeld Aktionen.
    Zu jeder von Ihnen erstellten Alarmregel ist im Auswahlfeld **Aktionen** bereits ein Standardaktion vom Typ **Protokoll-Handlerkonfiguration** enthalten. Wenn Sie andere Aktionen hinzufügen möchten, wie beispielsweise eine E-Mail senden, müssen Sie eine Aktion definieren und sie auf das Aktionsfeld ziehen.
11. Klicken Sie in der linken Spalte auf **Uhrzeit**. Ziehen Sie **Immer** aus der Zeitliste auf das Feld **Uhrzeit**.
12. Klicken Sie neben den Auswahlfeldern auf **OK**, um die Regel zu speichern, und klicken Sie dann bei der Erfolgsmeldung ebenfalls auf **OK**.
    Sie haben jetzt eine Alarmregel erstellt, die Teil des Regelsatzes ist. Wenn Sie Ihre Änderungen speichern möchten, müssen Sie den Regelsatz veröffentlichen.

13. Klicken Sie in der rechten Spalte auf die Schaltfläche **Veröffentlichen**.
    Sie können zur Seite **Regelübersicht** zurückgehen, um die Regel anzuzeigen und ggf. zu bearbeiten.
14. Klicken Sie in der linken Spalte auf **Regelübersicht**.
    Beachten Sie, dass hier zwei Regeln aufgelistet sind. Eine gehört zu der Regel, die Sie erstellt haben (mit einer **Alarm in lokales Ereignisprotokoll protokollieren**-Aktion) und die andere ist eine Standardregel, die Alarmbenachrichtigungen an den Coreserver sendet (mit einer Aktion vom Typ **Protokoll-Handlerkonfiguration**). Sie wird automatisch für jede Ihrer definierten Regeln erstellt, damit alle Alarme auf dem Coreserver protokolliert werden. Sie können diese Regel nicht löschen, es sei denn, Sie löschen alle Regeln für einen Alarm.
15. Wählen Sie die Regel **Standardmäßige Festplattennutzung** mit der Aktion **Alarm in lokales Ereignisprotokoll protokollieren** und klicken dann in der rechten Spalte auf **Regeln > Bearbeiten**.
    Verwenden Sie dieses Dialogfeld zum Ändern der Einstellungen der Regel.
16. Um die mit der Regel verknüpften Aktionen zu ändern, wählen Sie eine neue Option aus der Dropdownliste **Aktion** aus.
17. Um die Uhrzeit zu ändern, zu der die Alarmregel aktiv ist, wählen Sie eine neue Option aus der Dropdownliste **Uhrzeit** aus.
18. Um die Schweregrade für Alarmbenachrichtigungen zu ändern, klicken Sie auf die **Zustand**ssymbole.
    Ein abgeblendetes Symbol ist inaktiv, wenn Sie also nur Alarmmeldungen für kritische Zustandsalarme erhalten wollen, müssen Sie auf das Symbol "Warnung" (Status 2) (ein gelbes Dreieck) klicken, um es zu deaktivieren.
19. Markieren Sie das Kästchen **Zustand**, um die Laufwerkspeichernutzung als Alarm für den Zustand des Geräts einzubeziehen.
20. Klicken Sie auf **OK**. Die von Ihnen vorgenommenen Änderungen spiegeln sich jetzt in der Liste **Regelübersicht** wieder.
    Um die für diesen Regelsatz vorgenommenen Änderungen zu speichern, müssen Sie in erneut veröffentlichen. Dann wird er gespeichert und steht zur Bereitstellung auf Ihrer Regelsatzliste zur Verfügung.
21. Klicken Sie in der rechten Spalte auf **Veröffentlichen**.

Wenn Sie zur Management Console zurückkehren, wir Ihr neu erstellter Regelsatz unter **Alarmregelsätze** aufgeführt.

Erstellen eines Alarmregelsatzes

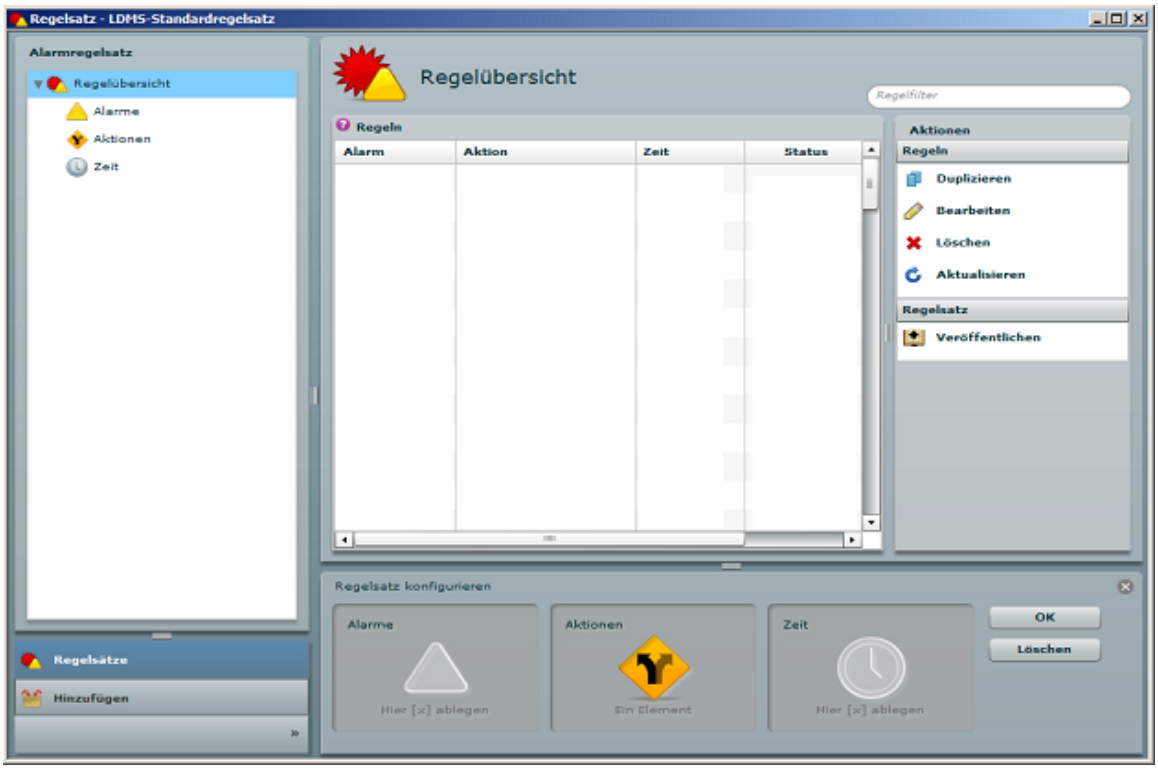
1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Klicken Sie in der Symbolleiste auf **Neuer Alarmregelsatz**. Geben Sie einen Namen ins Feld **Name** ein, eine Beschreibung des Alarms im Feld **Beschreibung** und klicken dann auf **OK**.
3. Um den Namen oder die Beschreibung des Regelsatzes zu ändern, wählen Sie in in der Liste **Alarmregelsätze** aus und klicken dann auf die Schaltfläche **Alarmregelsatz bearbeiten**.
4. Um einen Regelsatz zu kopieren, damit Sie daran kleinere Änderungen vornehmen können, klicken Sie mit der rechten Maustaste auf den Regelsatz in der Liste und wählen **Kopieren**. Geben Sie einen neuen Namen und eine neue Beschreibung ein und klicken Sie auf **OK**.

Wenn Sie einen Regelsatz erstellt haben, bearbeiten Sie den Regelsatz dahingehend, dass Sie Alarme und damit verknüpfte Aktionen hinzufügen.

Bearbeiten eines Alarmregelsatzes

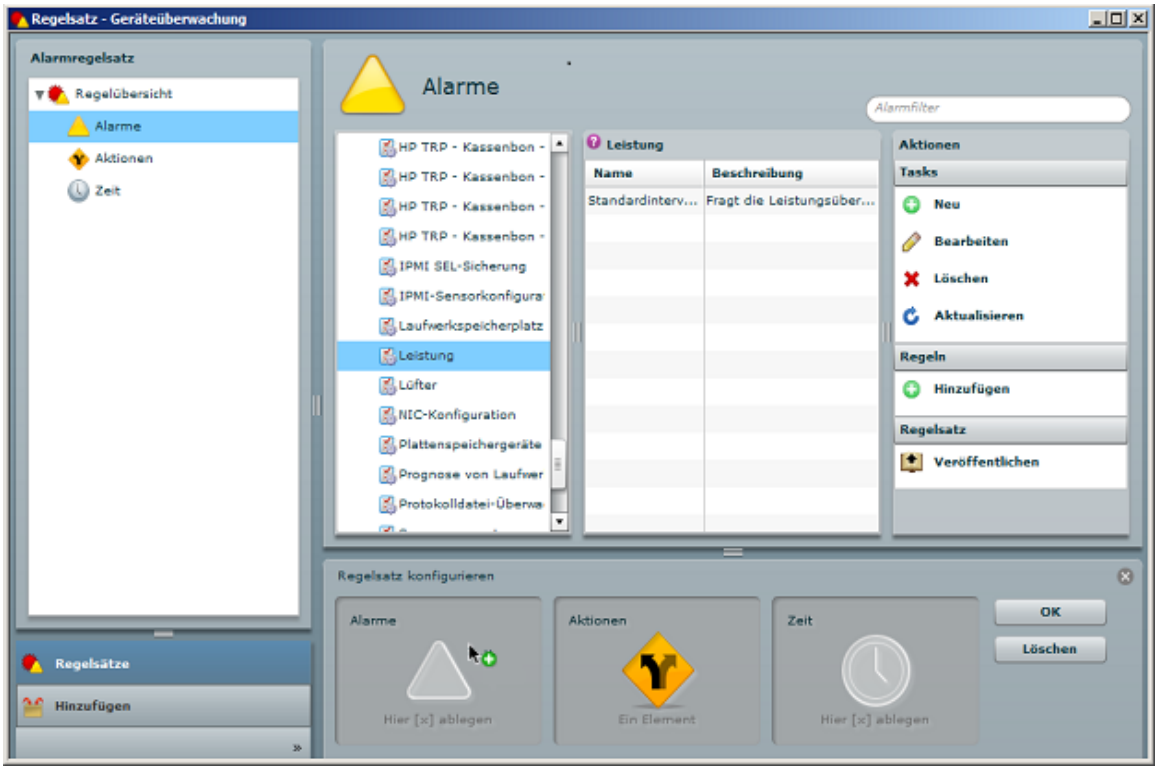
1. Markieren Sie in der Liste **Alarmregelsätze** den Regelsatz und klicken Sie dann in der Symbolleiste auf **Bearbeiten**.

   Auf der Seite Regelübersicht werden sämtliche Alarme im Regelsatz mit den verknüpften Aktionen und der Zeit aufgelistet. Jede Kombination aus Alarm, Aktion und Uhrzeit wird als separates Element in der Regelübersicht aufgeführt.



2. Klicken Sie in der linken Spalte auf **Alarme**, um dem Regelsatz eine Alarmregel hinzuzufügen.

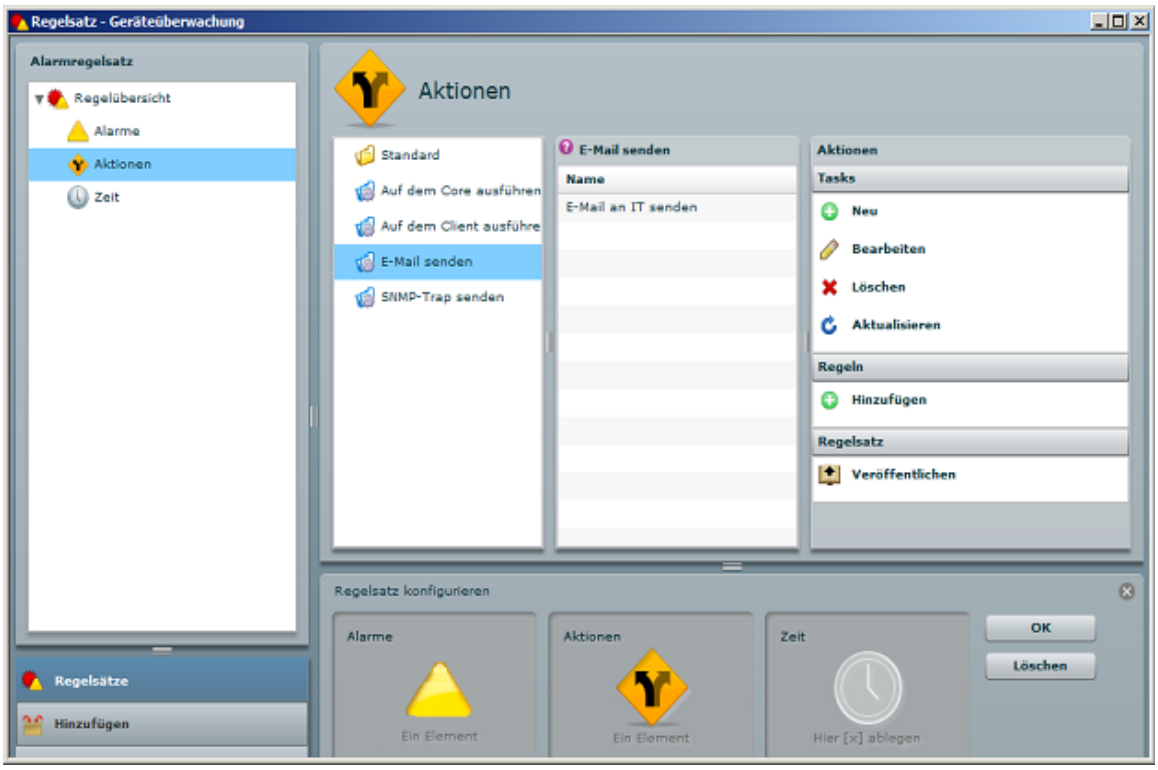
3. Klicken Sie in der rechten Spalte **Regeln > Hinzufügen**. Unten auf der Seite sind drei Auswahlfelder zur Verknüpfung von Alarmen, Aktionen und Zeitregeln dargestellt. Ziehen Sie einen Alarm aus der Liste auf den Auswahlbereich **Alarme** am unteren Rand der Seite.



Alarme sind in zwei Gruppen aufgelistet: **Standard** und **Überwachen**. Klicken Sie auf einen Punkt unter einer dieser Gruppen, um eine Gruppe der verknüpften Alarme anzuzeigen. Wenn Sie auf den Ordner **Alle Alarme** klicken, werden alle Alarme in alphabetischer Reihenfolge aufgeführt.

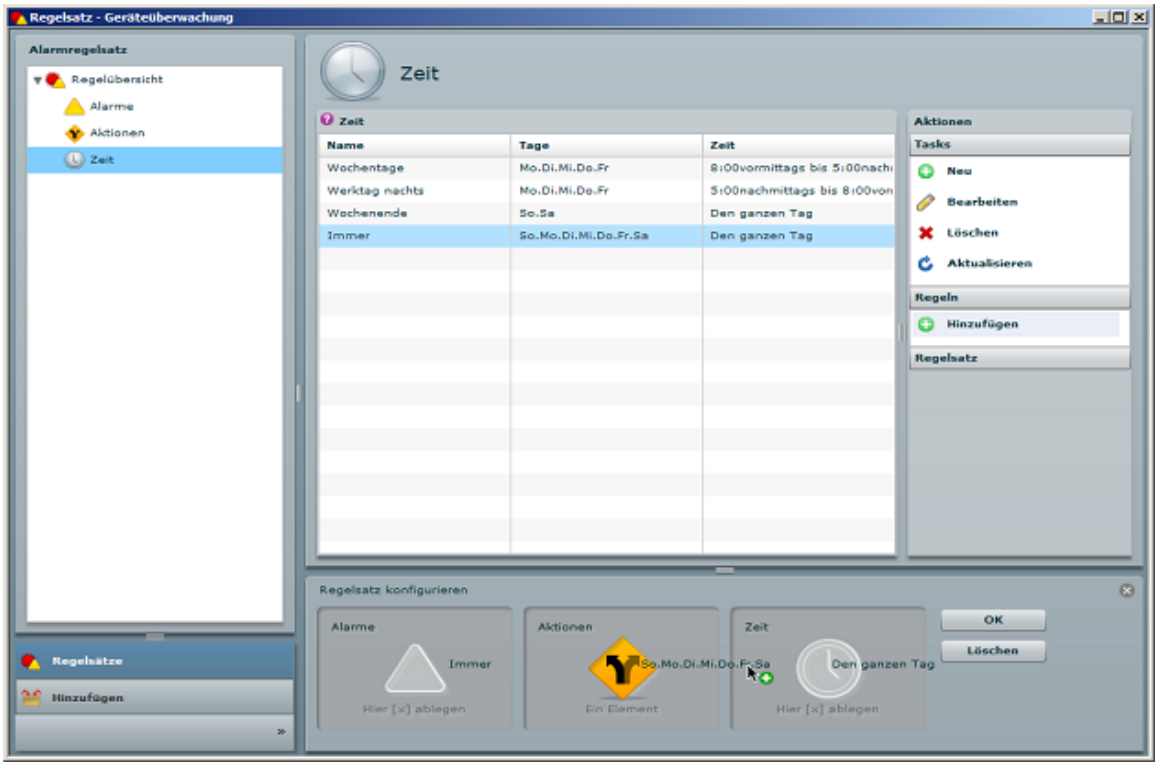
4. Um einen bestimmten Alarm zu suchen, geben Sie einen Suchbegriff in das Textfeld **Alarmfilter** rechts oben auf der Seite ein. Auf der Liste erscheinen alle Alarme, die die eingegebene Zeichenfolge enthalten.

5. Klicken Sie auf **Aktionen**, um eine Alarmaktion mit dem hinzugefügten Alarm zu verknüpfen. In der Grundeinstellung ist jedem Alarm eine **Log Handler-Konfiguration** zugeordnet, die den Alarm auf dem Coreserver protokolliert. Um eine weitere Aktion hinzuzufügen, ziehen Sie die Aktion auf das Feld **Aktionen** am unteren Seitenrand.



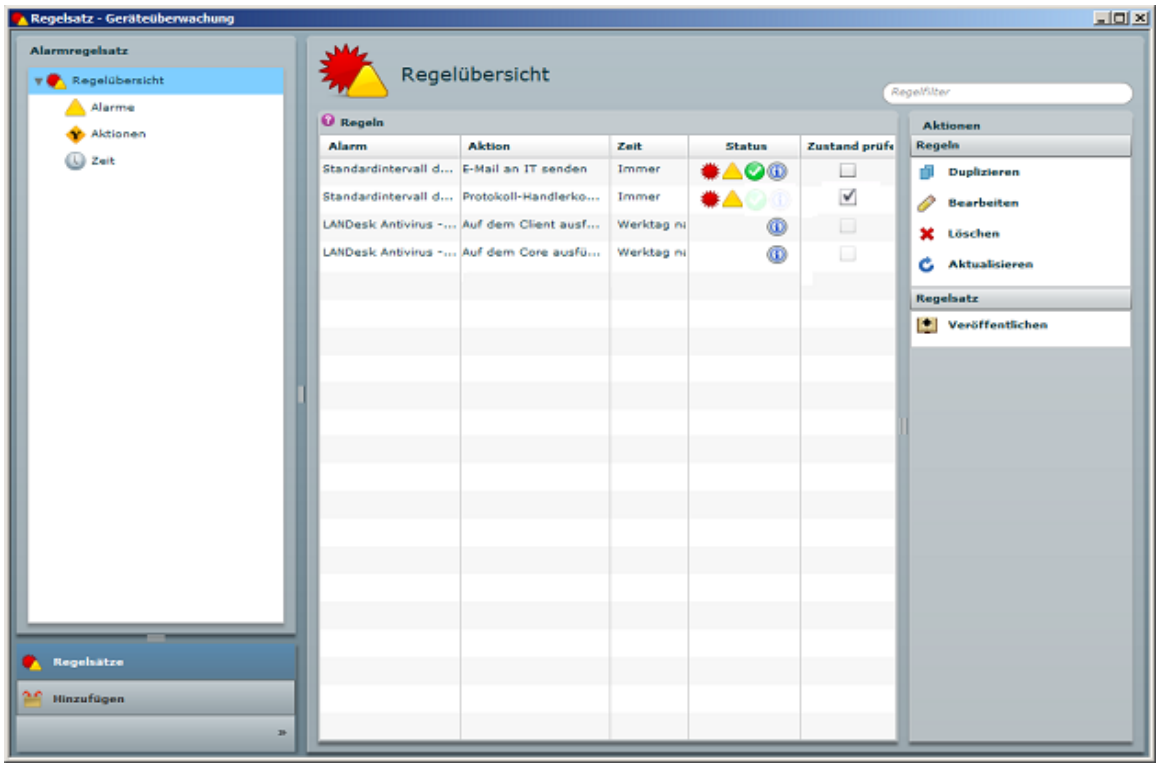
Der Ordner **Standard** enthält vordefinierte Aktionen. Um einen anderen Aktionstyp zu verwenden, müssen Sie zuerst die Aktion definieren.

6. Klicken Sie auf **Uhrzeit**, um anzugeben, wie oft ein Alarm überwacht werden soll. Ziehen Sie eine Zeitregel (z. B. **Immer**) auf das Feld **Uhrzeit** auf dem unteren Rand der Seite.



Standardmäßig stehen drei Zeitregeln zur Verfügung. Sie können bei Bedarf auch andere Zeitregeln definieren.

7. Wenn Sie mindestens einen Alarm mit einem zugeordneten Aktions- und Zeittask haben, klicken Sie auf die Schaltfläche **OK** unten auf der Seite und fügen Sie dem Regelsatz die Alarmregel hinzu. Klicken Sie nochmals auf **OK**.
8. Klicken Sie in der rechten Spalte auf die Schaltfläche **Veröffentlichen**.
9. Klicken Sie in der linken Spalte auf **Regelübersicht**, um den aktualisierten Regelsatz mit den neuen Alarmen anzuzeigen.



Auf der Liste von Alarmen im Regelsatz können Sie jeden Punkt einzeln bearbeiten, um die verknüpften Aktionen und Uhrzeiten zu ändern. Sie können auch auswählen, welcher Schweregrad für den Alarm gilt und angeben, ob der Alarm zum Gerätezustand beitragen soll oder nicht.

Details zum Definieren von Aktionen und Zeitfiltern sowie zum Bearbeiten von Regeleigenschaften finden Sie in den folgenden Themen.

Erstellen oder Bearbeiten eines Überwachungsalarms

Im Abschnitt "Überwachung" von Alarmen können Sie einen neuen Alarm definieren oder einen vorhandenen Überwachungsalarm bearbeiten, beispielsweise um das Abfrageintervall zu ändern.

1. Klicken Sie in der linken Spalte der Seite **Alarmregelsatz** auf **Alarme**.
2. Blättern Sie in der Strukturansicht nach unten zum Abschnitt **Überwachen**. Ein Alarm kann nur unter der Überschrift "Überwachen" erstellt oder bearbeitet werden.
3. Wählen Sie eine Kategorie aus (z. B. **Gehäuse**) und klicken dann in der rechten Spalte auf **Tasks > Neu**.
4. Fügen Sie bei Bedarf Informationen in die Felder **Name**, **Beschreibung** und **Abfrageintervall** ein und klicken Sie dann auf **OK**.

Der Alarm wird in der von Ihnen ausgewählten Kategorie aufgeführt und kann nun zu einem Regelsatz hinzugefügt werden.

Alarmaktionen definieren, die in den Regeln verwendet werden sollen

1. Klicken Sie in der linken Spalte der Seite **Alarmregelsatz** auf **Aktionen**.
2. Wählen Sie eine Aktionsgruppe aus (z. B. **E-Mail senden**) und klicken dann in der rechten Spalte auf **Tasks > Neu**.
3. Fügen Sie in den Feldern die gewünschten Informationen hinzu und klicken dann auf **Speichern**.

Die Aktion wird in der ausgewählten Gruppe aufgeführt und ist zum Verknüpfen mit Alarmen verfügbar. Erklärungen zu den Feldern in den verschiedenen Aktionstypen finden Sie nachstehend.

Auf dem Core ausführen/ Auf dem Client ausführen

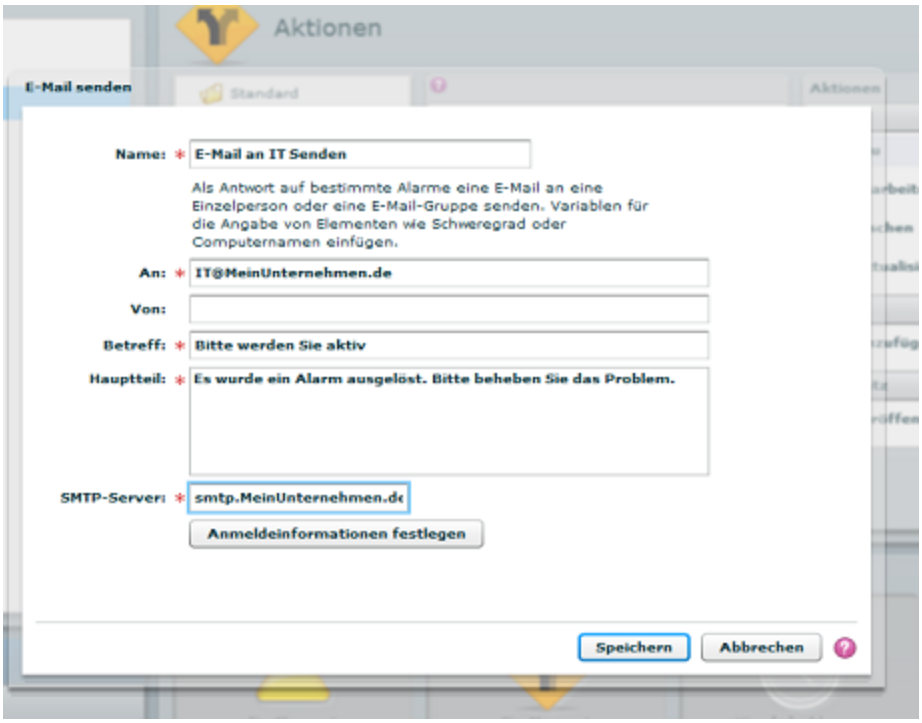
Diese Aktion startet entweder auf dem Coreserver oder auf dem verwalteten Gerät eine ausführbare Datei.

- **Name**: der bestimmende Name der Aktion. Seien Sie genau, sodass Sie die Aktionen einfach unterscheiden können.
- **Pfad und Dateiname**: der vollständige Pfad- und Dateiname der ausführbaren Datei, die auf dem Coreserver oder dem verwalteten Gerät ausgeführt werden soll. Wenn der Alarm ausgelöst wird, gibt der alarmierende Agent einen Befehl zum Ausführen dieser Datei aus.

Beachten Sie beim Auswählen einer der Aktionen, dass die Programme möglicherweise nicht wie erwartet auf dem Desktop angezeigt werden. Wenn die Anwendung ausgeführt wird, wird sie als Dienst in Windows gestartet und deshalb nicht so angezeigt wie eine reguläre Anwendung. Anwendungen, die auf diese Weise ausgeführt werden, sollten keine Benutzeroberfläche enthalten, die Eingaben erfordert. Um definitiv zu ermitteln, ob das Programm ausgeführt wurde, überprüfen Sie die Prozesse im Task-Manager von Windows.

E-Mail senden

Diese Aktion sendet über den von Ihnen angegebenen SMTP-Server eine E-Mail.



- **Name**: der bestimmende Name der Aktion. Seien Sie genau, sodass Sie die Aktionen einfach unterscheiden können.
- **An**: die vollständige E-Mail-Adresse der Person, die die E-Mail-Benachrichtigung erhalten soll.
- **Von**: eine beliebige, gültige E-Mail-Adresse, vorzugsweise eine, die darauf hinweist, dass es sich bei der E-Mail um eine Alarmbenachrichtigung handelt. Falls dies keine gültige E-Mail-Adresse ist, wird die Meldung auch nicht gesendet.
- **Betreff**: eine Beschreibung des Inhalts der E-Mail-Nachricht.
- **Hauptteil**: eine Meldung, die die Alarmbenachrichtigung begleitet.
- **SMTP-Server**: der Speicherort eines SMTP-Servers, von dem aus die E-Mail versendet werden kann.
- **Anmeldeinformationen festlegen**: anklicken, um einen Benutzernamen und ein Kennwort anzugeben, die zum Anmelden beim SMTP-Server verwendet werden können.

Die E-Mail wird vom Coreserver aus gesendet.

Sie können E-Mail-Meldungen an mehrere Empfänger senden und die folgenden Variablen im Textfeld verwenden:

- %% = %
- %D = Beschreibung
- %N = Computername
- %S = Schweregrad
- %T = Uhrzeit (UTC)

SNMP-Trap senden

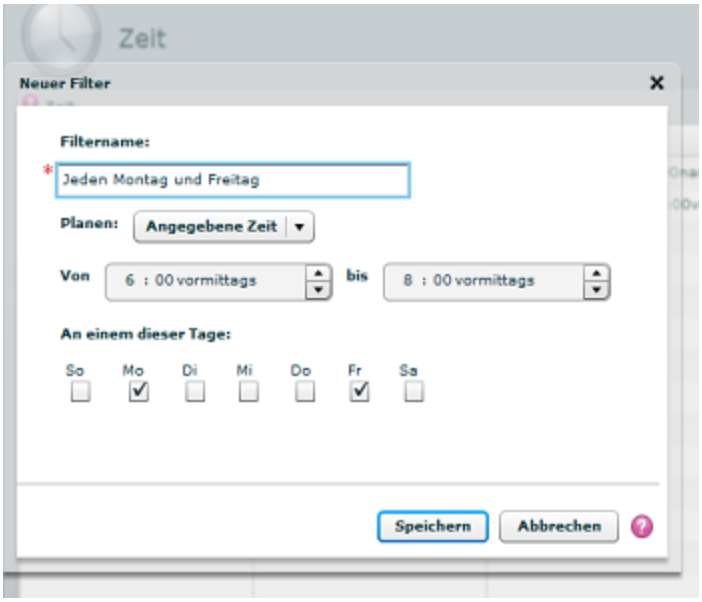
Diese Aktion sendet eine SNMP v1-Trap, wenn der Alarm ausgelöst wird.

- **Name**: der bestimmende Name der Aktion. Seien Sie genau, sodass Sie die Aktionen einfach unterscheiden können.
- **Hostname**: der Name des SNMP-Hosts, der den Trap empfängt.
- **Community-Zeichenfolge**: eine v1-Community-Zeichenfolge, die der Host zum Empfangen von Traps verwendet.

Die Schweregrade der Alarme werden im Feld "Bestimmter Trap-Typ" im Trap berichtet. Gültige Werte sind: 1 = unbekannt, 2 = Info, 3 = OK, 4 = Warnung, 5 = kritisch.

Zeitfilter definieren, die in den Alarmregeln verwendet werden sollen

1. Klicken Sie in der linken Spalte der Seite **Alarmregelsatz** auf **Zeit**.
2. Klicken Sie auf **Tasks > Neu** in der rechten Spalte.
3. Geben Sie im Dialogfeld **Neuer Filter** die Daten in die Felder ein (nachstehend beschrieben).
4. Klicken Sie auf **Speichern**.



Der Zeitfilter erscheint auf der Liste und kann nun mit den Alarmen verknüpft werden. Folgende Felder sind im Dialogfeld **Neuer Filter** enthalten:

- **Filtername**: der bestimmende Name der Aktion.
- **Planen**: Wählen Sie **Angegebene Zeit** für einen Filter, der die Uhrzeit und die Tage beschränkt, an denen der Alarm überwacht wird. Wählen Sie **Jederzeit**, um den Alarm ständig zu überwachen.
- **Von** und **Bis**: Wählen Sie einen Anfangs- und Endzeitpunkt am Tag, wenn der Alarm überwacht werden soll.
- **An einem dieser Tage**: Wählen Sie hier aus, an welchen Tagen der Alarm überwacht werden soll.

Bearbeiten einer Alarmregel

Auf der Seite **Regelübersicht** können Sie einzelne Alarmregeln bearbeiten. Mögliche Änderungen sind u.a. die Auswahl einer anderen Aktion oder eines anderen Zeitfilters, die Auswahl der zutreffenden Schweregrade und die Angabe, ob die Regel zum Gerätezustand beiträgt.

1. Klicken Sie auf **Regelübersicht**, um die Alarmregeln im aktuellen Regelsatz anzuzeigen.
2. Klicken Sie auf die Alarmregel, die Sie bearbeiten möchten und dann in der rechten Spalte auf **Regeln > Bearbeiten**.
3. Um die verknüpften Aktionen oder die Zeit zu ändern, wählen Sie eine neue Option aus der Dropdownliste aus.
4. Um nur für gewisse Schweregrade eine Alarmbenachrichtigung zu erhalten, klicken Sie auf die **Status**-Symbole. Ein abgeblendetes Symbol zeigt an, dass Alarme mit diesem Schweregrade ignoriert werden.
5. Um die Alarmregel als Anzeiger für den Gerätezustand einzubeziehen, markieren Sie das Kästchen **Zustand**.
6. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Duplizieren einer Alarmregel

Sie können jeder Alarmregel nur eine Aktion und einen Zeitfilter zuordnen. Wenn Sie zusätzliche Regeln für einen Alarm erstellen möchten, klicken Sie auf **Klonen** in der rechten Spalte, um ein Duplikat der Regel anzufertigen, das Sie dann bearbeiten können.

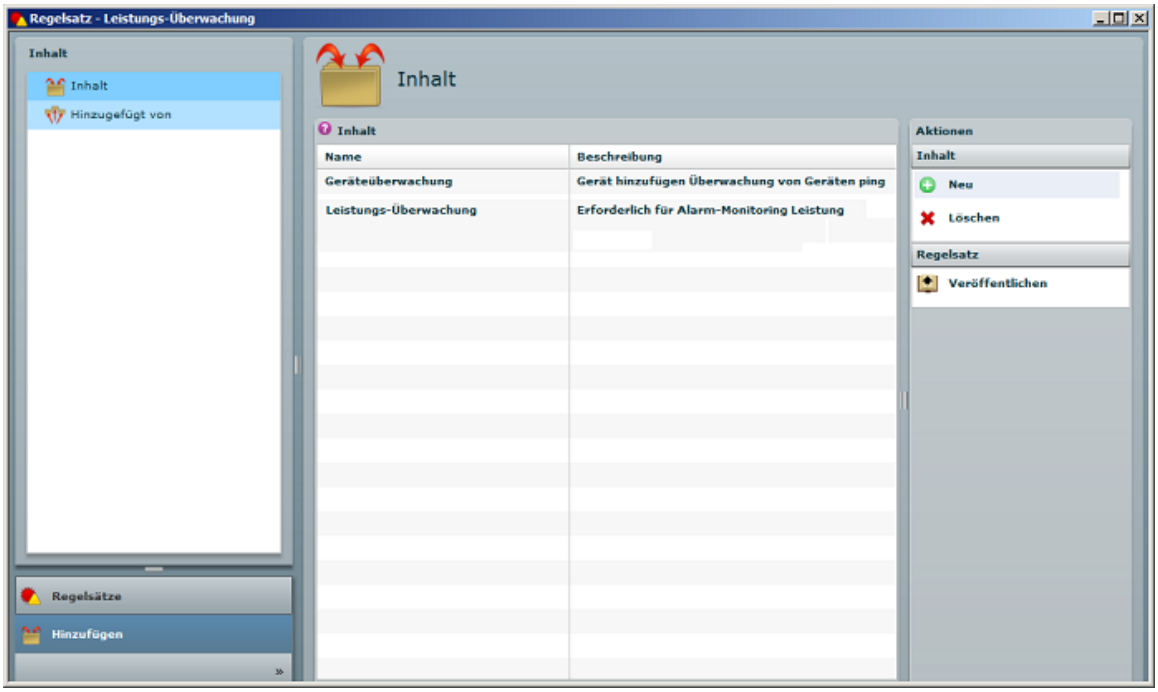
Regelsätze in andere Regelsätze einschließen

Eine Art, die Regelsatzerstellung flexibler zu gestalten, ist kleinere Regelsätze zu erstellen, die Sie dann für verschiedene Benutzer kombinieren können. Hierfür können Sie Regelsätze in andere Regelsätze einschließen.

1. Klicken Sie unten links auf der Seite **Alarmregelsatz** auf die Schaltfläche **Inhalt**.
2. Klicken Sie in der linken Spalte auf **Inhalt**.
3. Klicken Sie in der rechten Spalte auf **Inhalt > Neu**.
4. Wählen Sie im Dialogfeld **Verfügbare Regelsätze** mindestens einen Regelsatz aus, den Sie in den aktuellen Regelsatz einschließen möchten, und klicken auf **Speichern**. Verwenden Sie Strg + Klick oder Umschalt + Klick zur Auswahl mehrerer Regelsätze.

   Die Regelsätze werden zur Liste **Inhalt** hinzugefügt.

5. Wenn Sie einen Regelsatz aus der Liste **Inhalt** entfernen möchten, wählen Sie ihn aus und klicken in der rechten Spalte auf **Inhalt > Löschen**.
6. Um anzuzeigen, in welchen anderen Regelsätzen der aktuelle Regelsatz noch enthalten ist, klicken Sie in der linken Spalte auf **Hinzugefügt von**.



Wenn Sie Regelsätze einfügen, wird jeder einzelne Regelsatz als individuelle XML-Datei verwaltet. Die XML-Dateien werden nicht kombiniert, aber verweisen aufeinander.

Veröffentlichen eines Alarmregelsatzes

Nachdem Sie Regeln hinzugefügt und bearbeitet haben, müssen Sie den Regelsatz veröffentlichen. Dadurch entsteht eine XML-Datei mit den Regelsatzdaten, auf die sich der Alarmagent beim Ablauf bezieht.

1. Klicken Sie auf der Seite **Regelübersicht** auf die Schaltfläche **Veröffentlichen** in der rechten Spalte.
2. Klicken Sie bei der Erfolgsmeldung auf **OK**.

Die XML-Dateien mit veröffentlichten Regelsatzdaten werden im Ordner "Alarmregeln" im der Idlogon-Teil auf dem Coreserver gespeichert.

Wenn Sie einen Regelsatz veröffentlichen, wird der Alarmservice benachrichtigt, die aktualisierten Regelsätze neu zu laden. Wenn Sie einen Regelsatz aktualisieren, den Sie bereits auf verwalteten Geräten bereitgestellt haben, aktualisiert jedes dieser Geräte seine Regelsätze mit den geänderten Regeln automatisch, wenn der Alarmagent das nächste mal auf diesen Geräten ausgeführt wird.

Wenn Sie einen Regelsatz nicht veröffentlichen, wird kein Signal zum Alarmservice gesendet, um den Regelsatz neu zu laden, daher wird auch keine automatische Regelsatzaktualisierung auf den Geräten durchgeführt, auf denen dieser Regelsatz bereits vorhanden ist. Wir empfehlen Ihnen dringend, die Regelsätze jedes Mal zu veröffentlichen, wenn Sie Änderungen daran vornehmen.

Informationen zur Leistungsüberwachung

Management Suite unterstützt mehrere Methoden zur Überwachung des Systemzustands eines Geräts. Während Alarmregelsätze auf der Corekonsole definiert und auf mehreren Geräten bereitgestellt werden, können Sie auf einzelnen Geräten auch Leistungsüberwachungszähler zur Überwachung bestimmter Leistungspunkte definieren.

Sie können diese Leistungszähler definieren und sie verschiedene Datenarten auf Ihren Geräten überwachen lassen, z. B.:

- Hardwarekomponenten (z. B. Laufwerke, Prozessoren und Speicher)
- Hardwaresensoren (z. B. für Lüfter, Spannungswerte und Temperaturen)
- Betriebssystemkomponenten (z. B. Prozesse und Dienste)
- Anwendungskomponenten (z. B. die vom Webserver des Systems übertragenen Bytes pro Sekunde)
- Verwendungsstufen

Beim Auswählen eines Leistungszählers geben Sie auch das Abfrageintervall für das betreffende Element an, definieren Grenzwerte für die Leistung und legen fest, wie oft die Grenzwerte überschritten werden dürfen, ehe ein Alarm generiert wird. Nachdem Sie einen Leistungszähler definiert haben, können Sie in der Echtzeitinventar- und -überwachungskonsole die Seite **Überwachung** aufrufen und eine Übersicht Ihrer überwachten Alarme anzeigen.

Damit Sie auf die Leistungsüberwachungselemente eines Geräts aufmerksam gemacht werden können, müssen Sie eine Leistungsüberwachungsregel im Regelsatz für das Gerät einschließen.

Prozess zur Überwachung der Leistung von Elementen auf Geräten

Zur Überwachung der Leistung der verschiedenen Elemente auf Ihren verwalteten Geräten führen Sie die folgenden drei allgemeinen Tasks aus:

- Installieren eines Überwachungsagenten auf Geräten
- Erstellen von Leistungsüberwachungsregeln für einzelne Geräte

- Anzeigen von Leistungsüberwachungsdaten

Hinweise

- Wenn Sie Geräte einfach regelmäßig pingen möchten, um Ihre Konnektivität zu überwachen, verwenden Sie die Geräteüberwachungsfunktion.
- Die Kommunikation mit dem Überwachungsagenten erfolgt über HTTP over TCP/IP in Form von GET- oder POST-Anforderungen. Antworten auf Anforderungen befinden sich in XML-Dokumenten.
- Wenn Sie eine Abfrage zum Zustand eines Geräts (Computer.Health.State) ausführen und speichern, wird der Zustand in der Datenbank durch eine Ziffer repräsentiert. Die Ziffern entsprechen folgenden Zuständen: 4=Kritisch, 3=Warnung, 2=Normal, 1=Zu Informationszwecken, Null oder 0=unbekannt.
- Die Hardwareüberwachung ist von der Funktionalität der auf dem Gerät installierten Hardware sowie von der korrekten Konfiguration der Hardware abhängig. Wenn z. B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden keine Überwachungsdaten bereitgestellt.
- Wenn Sie den Eindruck haben, dass die Berichterstellung von einem bestimmten Rechner gestoppt wurde, können Sie mithilfe von "restartmon.exe" im Ordner LDCLIENT den Collector und alle Überwachungsanbieter neu starten. Dieses Dienstprogramm ist für Rechner gedacht, auf denen die Berichterstellung installiert wurde, jedoch keine Berichte mehr erstellt werden. Starten Sie mit diesem Dienstprogramm die Collector und Provider neu, ohne das Gerät neu starten zu müssen.

Verwandte Themen

"Grundlagen der Alarmierung" auf Seite 836

"Überwachen von Geräten auf Netzwerkkonnektivität" auf Seite 834

Bereitstellen eines Überwachungsagenten auf Geräten

Wenn der Echtzeitinventar- und Überwachungsagent auf dem Gerät installiert ist, stellt Management Suite eine sofortige Zusammenfassung zum Systemzustand des Geräts zur Verfügung. Der Überwachungsagent ist eine der Agentenkomponenten, die auf verwalteten Geräten installiert werden können.

Der Echtzeitinventar- und Überwachungsagent überprüft die Hardware und die Konfiguration eines Geräts in regelmäßigen Abständen und schreibt alle etwaigen Änderungen in den Systemstatus des Geräts. Der Status des Geräts wird auf dreierlei Weise angezeigt:

- durch das Statussymbol in der Liste **Geräte** der Netzwerkansicht
- durch den im Health-Dashboard angezeigten Zustand. (Klicken Sie auf **Extras > Berichte/Überwachung > Health Dashboard**.)
- durch Daten, die im Dashboard "Echtzeitinventar und Überwachung" für das Gerät angezeigt werden. (Klicken Sie mit der rechten Maustaste auf das Gerät in der Netzwerkansicht und wählen Sie **Echtzeitinventar und Überwachung** aus.)

Ein überwachtes Gerät, dessen Festplattenspeicher zunehmend knapper wird, kann das Symbol für eine "Warnung" einblenden, sobald die Festplatte zu 90% ausgelastet ist, und dieses Symbol in das Symbol für den Zustand "Kritisch" ändern, sobald die Auslastung 95% erreicht. Wenn das Gerät über einen Alarmregelsatz mit Leistungsüberwachungsregeln für einen Laufwerkspeicheralarm verfügt, erhalten Sie eventuell für denselben Festplattenstatus auch Alarmmeldungen.

Verwandte Themen

Konfigurieren von Geräteagenten

Erstellen von Leistungsüberwachungsregeln

Sie können entscheiden, welche Leistungselemente auf einem Gerät überwacht werden, indem Sie einen Überwachungsregelsatz definieren, der festlegt, was der Überwachungsagent auf dem Gerät überprüft. Hierfür müssen Sie auf dem Gerät einen Regelsatz bereitstellen, der eine Leistungsüberwachungsalarmregel enthält.

Es gibt viele Leistungszähler, die überwacht werden können. Beim Erstellen einer Leistungsüberwachungsregel können Sie jedes dieser Elemente ein- oder ausschalten, angeben, wie oft das Element überprüft werden soll, und für bestimmte Elemente Leistungsgrenzwerte festlegen. Sie können zudem auf dem Gerät ausgeführte Dienste überwachen lassen.

Der Prozess für das Erstellen von Leistungsüberwachungsregeln sieht wie folgt aus:

1. Fügen Sie die Leistungsüberwachung als Regel in den Alarmregelsatz des Geräts ein.
2. Stellen Sie den Regelsatz auf den Geräten bereit. (Sie können mehrere Geräte bestimmen, auf denen Sie den Regelsatz bereitstellen, müssen aber dann die Leistungsüberwachung auf einzelnen Geräten definieren.)
3. Erstellen Sie Leistungsüberwachungsregeln auf den Geräten mithilfe der Konsole "Echtzeitinventar und Überwachung". Einige Ereignisse, z. B. Dienste, setzen voraus, dass Sie jeden zu überwachenden Dienst einzeln auswählen (siehe ausführliche Beschreibung weiter unten).

So wählen Sie einen zu überwachenden Leistungszähler aus

1. Klicken Sie auf **Tools > Berichte / Überwachung >Tools > Health Dashboard**.
2. Doppelklicken Sie in der Liste der Geräte auf das Gerät, das Sie konfigurieren möchten.
   In einem anderen Browserfenster wird die Konsole "Echtzeitinventar und Überwachung" geöffnet.
2. Klicken Sie im linken Navigationsfenster auf **Überwachung**.
3. Klicken Sie auf die Registerkarte **Einstellungen für die Leistungszähler**.
4. Wählen Sie in der Spalte **Objekte** das zu überwachende Objekt aus.
5. Wählen Sie in der Spalte **Instanzen** ggf. die Instanz des zu überwachenden Objekts aus.
6. Wählen Sie in der Spalte **Zähler** den zu überwachenden Zähler aus.
2. Wenn der gewünschte Zähler nicht auf der Liste aufgeführt wird, klicken Sie auf **Zähler neu laden**, um die Liste mit etwaigen neuen Objekten, Instanzen oder Zählern zu aktualisieren.
7. Geben Sie das Abfrageintervall an (**alle *n* Sekunden**) und die Anzahl von Tagen, die der Zählerverlauf gespeichert werden soll.
8. Geben Sie im Feld **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** an, wie oft der Zähler die Grenzwerte überschreiten darf, ehe ein Alarm generiert wird.
9. Geben Sie die unteren und/oder oberen Grenzwerte an.
10. Klicken Sie auf **Übernehmen**.

Hinweise

- Protokolldateien können rasch an Volumen zunehmen. Allein durch das Abfragen eines einzelnen Zählers im Zwei-Sekunden-Intervall wächst das Leistungsprotokoll täglich um 2,5 MB.
- Eine Warnmeldung wird generiert, wenn ein Leistungszähler auf einem Windows- oder einem Linux-Gerät unter einen Grenzwert fällt. Wenn ein Leistungszähler auf einem Linux-Gerät einen oberen Grenzwert überschreitet, wird eine Warnmeldung generiert. Wenn ein Leistungszähler auf einem Windows-Gerät einen oberen Grenzwert überschreitet, wird eine kritische Warnung generiert.

- Berücksichtigen Sie beim Einrichten von Grenzwerten, dass Alarme generiert werden, ganz gleich, ob ein oberer oder unterer Grenzwert überschritten wird. Bei einem Grenzwert, der sich auf die verfügbare Speicherplatzmenge bezieht, möchten Sie wahrscheinlich nur benachrichtigt werden, wenn der Speicherplatz knapp wird. In diesem Fall, sollten Sie den oberen Grenzwert so hoch setzen, dass Sie nicht benachrichtigt werden, wenn auf dem Gerät eine große Menge Speicherplatz verfügbar wird.
- Indem Sie den Wert für **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** ändern, können Sie die Aufmerksamkeit auf ein hartnäckiges Problem oder ein isoliertes Ereignis lenken. Wenn Sie beispielsweise die von einem Webserver gesendeten Byte überwachen, kann Management SuiteSie alarmieren, wenn der Byte/Sek.-Wert konstant überhöht ist. Oder Sie können einen niedrigen Wert wie 1 oder 2 angeben, um eine Alarmnachricht zu erhalten, sobald Ihre anonymen FTP-Verbindungen eine bestimmte Anzahl von Benutzern überschreiten.
- Wenn Sie Dienste in einer Überwachungsregel bearbeiten, zeigt die Liste der **Verfügbaren Dienste** bekannte Dienste aus der Inventardatenbank an. Es werden keine Dienste im Listenfeld **Verfügbare Dienste** angezeigt, bis ein LANDesk Agent auf einem oder mehreren Geräten bereitgestellt und ein Inventarscan an den Core zurückgegeben wird. Wenn Sie z. B. einen Linux-Dienst in der Liste auswählen möchten, müssen Sie zunächst einen Agenten auf einem Linux-Gerät bereitstellen.

Generieren einer XML-Datei für einen Regelsatz

Als Teil des Bereitstellungsprozesses wird eine XML-Seite erstellt, die den bereitgestellten Regelsatz und die Geräte, auf denen der Regelsatz bereitgestellt wurde, auflistet. Dieser Bericht wird auf dem Coreserver im Ldlogon-Verzeichnis gespeichert und mit einer fortlaufenden Nummer benannt, die ihm von der Datenbank zugewiesen wird.

Wenn Sie diese XML-Seite unabhängig vom Bereitstellen eines Regelsatzes anzeigen möchten, klicken Sie auf die Schaltfläche **XML generieren** und klicken dann auf die Verknüpfung, mit der die XML-Datei angezeigt wird. Die Generierung eines Regelsatzes als XML-Datei hat zudem den Vorteil, dass der Regelsatz in der Liste der verfügbaren Regelsätze in den Einstellungen für die **Agentenkonfiguration** dargestellt werden kann.

Anzeigen von Leistungsüberwachungsdaten

Auf der Seite **Überwachung** können Sie die Leistung unterschiedlicher Systemobjekte überwachen. Sie können spezifische Hardwarekomponenten (Laufwerke, Prozessoren und Speicher) oder Betriebssystemkomponenten (Prozesse oder vom Webserver des Systems übertragene Byte/Sek.) überwachen. Die Seite **Überwachung** enthält ein Diagramm, das Echtzeitdaten oder Vergangenheitsdaten für Zähler anzeigt.

Um einen Leistungszähler zu überwachen, müssen Sie den Zähler zunächst auswählen. Hierbei wird der Zähler in die Liste der überwachten Zähler eingefügt. Bei diesem Vorgang geben Sie auch die Polling-Häufigkeit für das betreffende Element an, definieren Grenzwerte für die Leistung und legen fest, wie oft die Grenzwerte überschritten werden dürfen, bevor ein Alarm generiert wird.

So zeigen Sie überwachte Leistungszähler an

1. Klicken Sie auf **Tools > Berichte / Überwachung > Health Dashboard**.
2. Doppelklicken Sie in der Liste der Geräte auf das Gerät, das Sie konfigurieren möchten.
   In einem anderen Browserfenster wird die Konsole "Echtzeitinventar und Überwachung" geöffnet.
2. Klicken Sie in der Toolbox auf **Überwachung**.
3. Klicken Sie nach Bedarf auf die Registerkarte **Aktive Leistungszähler**.

4. Wählen Sie in der Dropdownliste **Zähler** den Zähler aus, für den Sie ein Leistungsdiagramm anzeigen möchten.
5. Wählen Sie **Echtzeitdaten** anzeigen aus, um ein Diagramm auf der Basis von Echtzeitdaten zur Leistung anzuzeigen.
6. Um ein Diagramm zur Leistung innerhalb eines bestimmten Zeitraums anzuzeigen, wählen Sie bei der Auswahl des Zählers **Vergangenheitsdaten anzeigen** (Verlauf behalten).

Hinweise

Im Leistungsdiagramm repräsentiert die Horizontalachse den verstrichenen Zeitraum. Die Vertikalachse repräsentiert die gemessenen Einheiten, beispielsweise Byte/Sek. (beim Überwachen von Dateiübertragungen), Prozent (beim Überwachen des Prozentsatzes der CPU-Nutzung) oder verfügbare Byte (beim Überwachen des Festplattenspeichers). Die Linienhöhe ist eine flexible Einheit. Die Höhe der Linie ändert sich je nach den Datenextremen; für den einen Zähler kann die Vertikalachse z. B. 1 bis 100 repräsentieren und für einen anderen vielleicht 1 bis 500.000. Bei Daten mit extremer Variationsbreite können minimale Änderungen als flache Linie erscheinen.

Die Spalten zu den überwachten Zähler enthalten Informationen darüber, wie oft die Zähler geprüft wurden, wie oft ein Zähler außerhalb des Bereichs war und ein Alarm gesendet wurde sowie die unteren und oberen Grenzwerte.

Beim Auswählen eines anderen Zählers wird das Diagramm aktualisiert und die Maßeinheit zurückgesetzt.

Wenn Sie einen Alarm erhalten, der von einem in der Liste geführten Zähler generiert wurde, klicken Sie mit der rechten Maustaste auf den Zähler und klicken auf **Bestätigen**, um den Alarm zurückzusetzen.

Beenden der Überwachung eines Leistungszählers

1. Klicken Sie auf **Extras > Berichte / Überwachung > Health Dashboard**.
2. Doppelklicken Sie in der Liste der Geräte auf das Gerät, das Sie konfigurieren möchten. In einem anderen Browserfenster wird die Konsole "Echtzeitinventar und Überwachung" geöffnet.
2. Klicken Sie in der Toolbox auf **Überwachung**.
3. Klicken Sie bei Bedarf auf die Registerkarte **Aktive Leistungszähler**.
4. Klicken Sie unter **Überwachte Leistungszähler** mit der rechten Maustaste auf den Zähler und klicken Sie auf **Löschen**.

Anzeigen des globalen Alarmprotokolls

Verwenden Sie die Seite **Alarmprotokoll** zum Anzeigen von Alarmen, die an den Coreserver gesendet wurden. Das Protokoll wird nach der Uhrzeit (GMT) sortiert, wobei sich der jüngste Alarm am Anfang des Protokolls befindet.

So zeigen Sie das globale Alarmprotokoll an

1. Klicken Sie auf **Tools > Berichte/Überwachung > Protokolle**.
2. Klicken Sie auf eine Spaltenüberschrift, um Einträge anhand der Spalte zu sortieren.
3. Doppelklicken Sie auf den Eintrag in der Spalte **Alarmname**, um eine ausführliche Beschreibung eines Alarms anzuzeigen.

4. Um Protokolleinträge nach Name, Status oder Instanz aufzulisten, wählen Sie die Filterkriterien in der Dropdownliste **In Spalte** aus. Wählen Sie beispielsweise **Alarmname** aus und geben Sie einen vollständigen Namen ein (beispielsweise "Leistung"); oder geben Sie mit dem Platzhalter * einen Teil eines Namens in das Feld **Suche** ein (beispielsweise "Remote*"). Um einen Suchvorgang nach dem Datum auszuführen, wählen Sie **Datumsfilter aktivieren** aus, geben einen Bereich mit einem Anfangs- und Enddatum ein. Wenn Sie Filterkriterien hinzugefügt haben, klicken Sie in der Symbolleiste auf **Suchen**.
5. Um den Zustandsstatus eines Alarms zu löschen, wählen Sie in der Spalte **Alarmname** den Alarm aus, klicken in der Symbolleiste auf die Schaltfläche **Bestätigen** und dann auf **OK**.
6. Um einen Protokolleintrag zu löschen, rechtsklicken Sie auf den Alarm und wählen **Löschen**.

HINWEIS: Wenn der Gerätename nicht als vollständig qualifizierter Domänenname angezeigt wird, so liegt das daran, dass das Produkt nicht in der Lage war, den vollständig qualifizierten Domänennamen für das Gerät aufzulösen.

Klicken Sie hier, um Beschreibungen der verschiedenen Spalten des Alarmprotokolls anzuzeigen.

- **Alarmname:** Der mit dem Alarm assoziierte Name - wie auf der Seite **Alarmkonfigurationen** definiert.
- **GMT-Zeit:** Datum und Uhrzeit der Alarmerstellung (GMT).
- **Status**: Der Schweregrad des Alarms, wobei folgende Statusangaben unterstützt werden:
  - **Unbekannt:** Der Status lässt sich nicht ermitteln.
  - **Zur Information:** Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen.
  - **OK:** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.
  - **Warnung:** Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
  - **Kritisch:** Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Gerätename:** Der Name des Geräts, auf dem der Alarm generiert wurde. Dies sollte ein vollständig qualifizierter Domänenname sein.
- **IP-Adresse:** Die IP-Adresse des Geräts, auf dem der Alarm generiert wurde.
- **Instanz:** Liefert detaillierte Informationen zu der Situation, in der der Alarm generiert wurde.

Anzeigen des Alarmprotokolls eines Geräts

Verwenden Sie die Seite **Alarmprotokoll** zum Anzeigen von Alarmen, die an ein verwaltetes Gerät gesendet wurden. Das Protokoll wird nach der Uhrzeit (GMT) sortiert, wobei sich der jüngste Alarm am Anfang des Protokolls befindet.

So zeigen Sie das Alarmprotokoll für ein bestimmtes Gerät an

1. Klicken Sie auf **Extras > Berichte/Überwachung > Health Dashboard**.
2. Doppelklicken Sie in der Liste der Geräte auf das Gerät.
3. Klicken Sie im linken Navigationsfenster auf **Systeminformationen**.
3. Klicken Sie auf **Protokolle > Alarmprotokoll**.
4. Um Einträge nach Uhrzeit, Name oder Status zu sortieren, klicken Sie auf eine Spaltenüberschrift.

5. Doppelklicken Sie auf den Eintrag in der Spalte **Alarmname**, um eine ausführliche Beschreibung eines Alarms anzuzeigen.
6. Um Protokolleinträge nach Name oder Status aufzulisten, klicken Sie auf die Schaltfläche **Filter** in der Symbolleiste und wählen Filterkriterien aus. Wählen Sie beispielsweise **Alarmname** aus und geben Sie einen vollständigen Namen ein (beispielsweise "Performance"); oder geben Sie mit dem Platzhalter * einen Teil eines Namens ein (beispielsweise Remote*). Um einen Suchvorgang nach dem Datum auszuführen, wählen Sie **Datumsfilter aktivieren** aus, geben einen Bereich mit einem Anfangs- und Enddatum ein. Wenn Sie die Filterkriterien hinzugefügt haben, klicken Sie auf **Suche.**
7. Um den Zustandsstatus eines Alarms zu löschen, wählen Sie in der Spalte **Alarmname** den Alarm aus, klicken in der Symbolleiste auf **Alarm bestätigen** und dann auf **OK**.
8. Um einen Protokolleintrag zu löschen, klicken Sie auf den Alarm in der Spalte **Alarmname** und dann in der Symbolleiste auf **Eintrag löschen**.

Sie können auch das Alarmprotokoll des Geräts anzeigen, indem Sie auf die Schaltfläche **Alarmprotokoll** auf der Seite **Regelsätze** der Konsole "Echtzeitinventar und Überwachung" klicken.

HINWEIS: Wenn der Gerätename nicht als vollständig qualifizierter Domänenname angezeigt wird, so liegt das daran, dass das Produkt nicht in der Lage war, den vollständig qualifizierten Domänennamen für das Gerät aufzulösen.

Klicken Sie hier, um Beschreibungen der verschiedenen Spalten des Alarmprotokolls anzuzeigen.

- **Alarmname:** Der mit dem Alarm assoziierte Name - wie auf der Seite **Alarmkonfigurationen** definiert.
- **GMT-Zeit:** Datum und Uhrzeit der Alarmerstellung (GMT).
- **Status**: Der Schweregrad des Alarms, wobei folgende Statusangaben unterstützt werden:
  - **Unbekannt:** Der Status lässt sich nicht ermitteln.
  - **Zur Information:** Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen.
  - **OK:** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.
  - **Warnung:** Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
  - **Kritisch:** Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Instanz:** Liefert detaillierte Informationen zu der Situation, in der der Alarm generiert wurde.

Überwachen des Inhalts von Protokolldateien

Die Protokolldatei-Überwachung ist eine Option, die in den Überwachungsregeln bereitgestellt wird. Dieser Überwachungsagent scannt Protokolldateien auf verwalteten Windows-Geräten auf spezifische Zeichenfolgen oder Ausdrücke, und generiert eine Alarmmeldung, wenn er diese vorfindet. Dies ist nützlich, wenn Sie beim Vorliegen einer bestimmten Bedingung, die sich mithilfe einer Protokolldatei nachverfolgen lässt, benachrichtigt werden möchten.

Sie können eine von einer Anwendung generierte Textdatei überwachen lassen, einschließlich .htm- und .xml-Dateien (Unicode-Dateien lassen sich jedoch nicht überwachen). Nachdem Sie die zu überwachende Datei angegeben und mithilfe regulärer Ausdrücke Regeln definiert haben, wird die Datei automatisch so lange überwacht, wie die Protokolldatei-Überwachungsregel in einem Regelsatz auf dem betreffenden Gerät gültig ist.

Wenn in der Protokolldatei enthaltener Text zum ersten Mal mit einem regulären Ausdruck übereinstimmt, wird eine Alarmmeldung generiert. Der Alarm wird nur einmal für diese Datei generiert, selbst wenn es mehrere Übereinstimmungen gibt. Wenn sich die Datei später ändert, sodass keine übereinstimmende Bedingung mehr vorliegt, beginnt der Agent erneut auf diesen regulären Ausdruck zu scannen und generiert einen Alarm beim nächsten Vorkommen der Übereinstimmung.

Sie können auch Backup-Dateien von Protokollen scannen. Diese Dateien werden angelegt, wenn eine Protokolldatei zu groß wird und ältere Einträge in der Datei an eine andere Datei angehängt werden ("rollierende" Protokolldatei). So genannte "Wrapping"-Protokolldateien, die ältere Einträge in der Protokolldatei löschen, um für neue Einträge Platz zu machen, werden nicht unterstützt.

Für diese Überwachungsoption müssen Sie das Verzeichnis und den genauen Namen der Datei auf dem verwalteten Gerät angeben. Darüber hinaus geben Sie die Suchkriterien mithilfe eines regulären Ausdrucks an. Sobald eine Zeichenfolge in der Datei mit dem Ausdruck übereinstimmt, wird eine Alarmaktion generiert, sofern Sie einen Alarm des Typs **Protokolldatei-Überwachung** im relevanten Alarmregelsatz definiert haben.

Sie können die Protokolldatei-Überwachung in jeden Alarmregelsatz einschließen, den Sie definiert haben. Die folgende Prozedur beschreibt die fünf allgemeinen Schritte für die Einstellung der Protokolldatei-Überwachung:

1. Erstellen Sie eine Protokolldatei-Überwachungsregel in einem Alarmregelsatz.
2. Geben Sie an, welche Protokolldateien auf den verwalteten Geräten zu überwachen sind.
3. Definieren Sie die Überwachungsregeln für diese Datei mithilfe regulärer Ausdrücke.
4. Wählen Sie einen Schweregrad für die Regel aus und benennen Sie die Instanz, damit sie in Alarmen erkannt werden kann.
5. Übernehmen Sie Aktionen und Zeitregeln und speichern Sie die Regel im Alarmregelsatz.

Hinweise

- Die Protokolldatei-Überwachung wird nur für verwaltete Windows-Geräte unterstützt.
- Jedes Mal, wenn Sie eine Regel bearbeiten oder löschen, müssen Sie den Alarmregelsatz, in dem diese Regel vorkommt, veröffentlichen. Die entsprechenden Änderungen werden nicht übernommen, bevor der Regelsatz veröffentlicht wurde (oder bis Sie den Regelsatz mithilfe eines geplanten Tasks neu bereitstellen).
- Diese Funktion ordnet Protokolldateien im Speicher zu, um auf diese Weise den Speicherbedarf während einer Suche zu reduzieren. Hierfür wird Runtime-Speicher den stattfindenden linearen (auf regulären Ausdrücken basierenden) Suchvorgängen zugewiesen. Da Windows die Datei sperrt, wenn sie im Speicher zugeordnet wird, können bei einigen Anwendungen Probleme auftreten.

Verwandte Themen

"Konfigurieren von Alarmregelsätzen" auf Seite 842

"Einrichten einer Protokolldatei-Überwachungsregel" auf Seite 863

Einrichten einer Protokolldatei-Überwachungsregel

1. Klicken Sie auf **Extras > Konfiguration > Alarmierung**.
2. Wählen Sie aus **Alarmregelsätze** den Regelsatz aus, den Sie bearbeiten möchten und klicken Sie dann in der Symbolleiste auf **Bearbeiten**.
3. Klicken Sie in der linken Spalte des Fensters **Alarmregelsatz** auf **Alarme**. Klicken Sie im Ordner **Überwachen** auf der Alarmliste auf **Protokolldatei-Überwachung**.
4. Klicken Sie auf **Tasks > Neu** in der rechten Spalte.
5. Geben Sie im Dialogfeld **Protokolldatei-Überwachung** einen Namen und eine Beschreibung der Protokolldatei-Überwachungsregel ein.
6. Um die Häufigkeit zu ändern, mit der das Element überwacht wird, ändern Sie die Einstellungen des **Polling-Intervalls**.
7. Klicken Sie auf **Protokolldateikonfiguration**, um anzugeben, welche Dateien überwacht werden, woraufhin diese überwacht werden und wie Sie alarmiert werden.
   Reguläre Ausdrücke werden zur Definition des zu überwachenden Inhalts der Protokolldatei verwendet. Wenn der Überwachungsservice eine Übereinstimmung der regulären Ausdrücke in der Protokolldatei findet, befolgt er die Alarmregeln, um Sie von dem Vorfall zu unterrichten.
8. Klicken Sie auf **Verwalten**. Fügen Sie im Dialogfeld **Verwaltung regulärer Ausdrücke** einen beschreibenden Namen und einen regulären Ausdruck hinzu und klicken dann auf **Hinzufügen**. Wiederholen Sie dies für jeden regulären Ausdruck, den Sie zur Überwachung der Protokolldateien verwenden möchten. Wenn Sie diese allesamt hinzugefügt haben, klicken Sie auf **OK.**
   Sie können in diesem Dialogfeld beliebig viele reguläre Ausdrücke verwenden. Beachten Sie, dass Sie eine neue Regel für jeden Ausdruck erstellen müssen, nach dem Sie suchen möchten und jede Regel nur in eine Protokolldatei übernommen werden kann. Mit anderen Worten: jede Regel enthält einen regulären Ausdruck und eine Protokolldatei.
9. Wählen Sie einen regulären Ausdruck aus der Dropdownliste **Regulärer Ausdruck** aus.
10. Geben Sie den Pfad und vollständigen Dateinamen der zu überwachenden Protokolldatei in das Feld **Protokolldateipfad** ein. Es muss sich dabei um einen bestimmten Dateinamen handeln und nur dieser Dateiname wird überwacht (z. B. c:\logs\error.txt)
11. Wenn Sie Sicherungsdateien für die Protokolldatei einschließen möchten, geben Sie den Pfad und vollständigen Dateinamen der Sicherungsdatei in das Feld **Backup-Protokolldateipfad** ein (dieser Schritt ist optional). Dies muss ebenfalls ein vollständiger Pfad und Dateiname für eine bestimmte Datei sein.
12. Geben Sie einen beschreibenden **Instanznamen** ein. Dadurch wird die Protokolldatei-Überwachungsregel in der Alarmbenachrichtigung erkannt, die Sie erhalten.
13. Wählen Sie den Schweregrad aus, den Sie mit dieser Alarmregel verknüpfen möchten.
14. Wenn Sie nur neue Einträge in die Protokolldatei überwachen möchten, (ab dem Zeitpunkt der Bereitstellung der Überwachungsregel auf dem Gerät), klicken Sie auf **Änderungen der Protokolldatei überwachen**. (Diese Option wird typischerweise für Protokolldateien verwendet, damit der Agent den bereits vorhandenen Text nicht wieder und wieder scannt.)
    Wenn Sie alle vorhandenen und alle neuen Einträge in der Protokolldatei überwachen möchten, klicken Sie auf **Gesamte Protokolldatei überwachen**. (Diese Option wird normalerweise verwendet, um andere, weniger dynamische Dateien zu überwachen, z. B. Konfigurationsdateien.)
15. Klicken Sie auf **OK**, um die Regel der Liste mit Protokolldatei-Überwachungsregeln hinzuzufügen.

16. Wiederholen Sie die Schritte 4 bis 15, um weitere Protokolldatei-Überwachungsregeln hinzuzufügen. Nachdem Sie die gewünschten Protokolldatei-Überwachungsregeln erstellt haben, müssen Sie diese zum Regelsatz hinzufügen. Sie können mehrere Überwachungsregeln hinzufügen und Aktions- und Zeitregeln auf sie anwenden, je nachdem, wie Sie benachrichtigt werden möchten, wenn die Protokolldatei einen Alarm auslöst.
17. Klicken Sie in den unter **Protokolldatei-Überwachung** aufgeführten Regeln auf **Regel > Neu** in der rechten Spalte.
    Es werden drei Kästchen oder Auswahlfelder am unteren Seitenrand dargestellt.
18. Ziehen Sie mindestens eine Regel ins Feld **Alarme**.
19. Klicken Sie in der linken Spalte auf **Aktionen** , dann ziehen Sie mindestens eine Aktionsregel in das Feld **Aktionen**. Die Aktionen, die Sie hier hinzufügen, werden in jede Regel übernommen, die Sie hinzufügen.
20. Klicken Sie in der linken Spalte auf **Uhrzeit** , dann ziehen Sie mindestens eine Aktionsregel in das Feld **Uhrzeit**.
21. Klicken Sie auf **OK**, um die neuen Regeln zur Liste hinzuzufügen.
    Um die neuen Protokolldatei-Überwachungsregeln im Regelsatz anzuzeigen, klicken Sie auf **Regelübersicht**. Jede Regel wird auf einer separaten Zeile angezeigt und Sie können einzelne Regeln bearbeiten oder eine Regel klonen und Kopien davon mit verschiedenen Aktionen, Zeitregeln oder Schweregradstatus machen. Wenn Sie möchten, dass die Alarmregel den Gerätezustand beeinflusst, doppelklicken Sie auf die Regel auf der Liste **Regelübersicht** und markieren Sie das Kästchen **Zustand**.
22. Nachdem Sie die Protokolldatei-Überwachungsregeln dem Regelsatz hinzugefügt haben, klicken Sie auf **Veröffentlichen**, um die Änderungen am Regelsatz zu speichern. Die Änderungen werden auf den einzelnen Geräten übernommen, wenn Sie den Regelsatz das nächste Mal bereitstellen oder wenn der Inventardienst des Geräts das nächste Mal ausgeführt wird.

Hinweise

- Die Protokolldatei-Überwachung wird nur für verwaltete Windows-Geräte unterstützt.
- Jedes Mal, wenn Sie eine Regel bearbeiten oder löschen, müssen Sie den Alarmregelsatz, in dem diese Regel vorkommt, veröffentlichen. Die entsprechenden Änderungen werden nicht übernommen, bevor der Regelsatz veröffentlicht wurde (oder bis Sie den Regelsatz mithilfe eines geplanten Tasks neu bereitstellen).
- Diese Funktion ordnet Protokolldateien im Speicher zu, um auf diese Weise den Speicherbedarf während einer Suche zu reduzieren. Hierfür wird Runtime-Speicher den stattfindenden linearen (auf regulären Ausdrücken basierenden) Suchvorgängen zugewiesen. Da Windows die Datei sperrt, wenn sie im Speicher zugeordnet wird, können bei einigen Anwendungen Probleme auftreten.

Konfigurieren von Dell OMCI-Geräten

Dieses Produkt umfasst eine Management-Integrationsfunktion für Geräte, auf denen die Dell OMCI-Software installiert ist. OMCI (OpenManage Client Instrumentation) ist eine Technologie für Dell-Geräte, die die Remoteverwaltung des Gerätestatus und der Geräteeinstellungen ermöglicht.

Wenn LANDesk Management Suite ein Dell-Gerät erkennt, das mit OMCI ausgestattet ist, wird im Menü **Konfigurieren** der Konsole ein OMCI-Extra aktiviert. Dies gibt Ihnen die Möglichkeit, OMCI für Änderungen an den BIOS-Einstellungen auf Dell OMCI-Geräten zu verwenden.

Der OMCI-Konfigurationsprozess

Wenn Sie das Extra "Dell OMCI-Konfiguration" aufrufen, entsprechen die aufgeführten Standardeinstellungen denen eines Dell OMCI-Geräts in Ihrer Liste **Alle Geräte**. Wenn Sie zuerst ein Gerät auswählen, werden die Einstellungen dieses Geräts dazu verwendet, die Liste der BIOS-Einstellungen aufzufüllen. Wenn Sie kein Gerät auswählen, verwendet das Extra die Einstellungen des ersten OMCI-Geräts, das es findet.

Im Dialogfeld zur Konfiguration der BIOS-Einstellungen sind die BIOS-Einstellungen aufgeführt, die Sie ändern können. Der aktuelle Status jeder Einstellung ist aufgeführt und Sie können in einer Spalte **Neue Einstellungen** andere Einstellungen auswählen. Darüber hinaus können Sie das BIOS-Kennwort und das BIOS-Assetkennzeichen ändern.

Nachdem Sie diese Einstellungen konfiguriert haben, werden diese als Softwareverteilungspaket gespeichert. Dieses Paket können Sie dann an ein oder mehrere Dell OMCI-Geräte verteilen, die von Ihnen verwaltet werden. Diese Einstellungen werden auf jedem Gerät als Agent gespeichert. Bei manchen Einstellungen erhalten Sie Alarmmeldungen, wenn sich der Gerätestatus ändert.

HINWEIS: Wenn Einstellungen, die Sie ändern möchten, nicht angezeigt werden, kann es unter Umständen sein, dass diese nicht auf dem Dell OMCI-Gerät verfügbar waren, das zum Auffüllen der Liste verwendet wurde. Versuchen Sie ein anderes verwaltetes Gerät auszuwählen und klicken Sie dann auf **Konfigurieren > Dell OMCI-Konfiguration**, um die Liste mit den Einstellungen des neuen Geräts aufzufüllen.

VORSICHT: Es gibt eine Vielzahl möglicher BIOS-Einstellungen, die mit diesem Extra konfiguriert werden können. In einigen Fällen kann es sein, dass BIOS-Einstellungen auf einem Gerät nicht im BIOS eines anderen Geräts zur Verfügung stehen. Achten Sie darauf, kompatible Geräte auszuwählen, wenn Sie eine Dell OMCI-Konfiguration erstellen und auf verschiedene Geräte verteilen. Wenn die Konfiguration BIOS-Einstellungen umfasst, die mit einem der Zielgeräte nicht kompatibel sind, kann dies zu unvorhergesehenen Ergebnissen führen.

So konfigurieren Sie die OMCI-Einstellungen für Dell-Geräte

1. Wenn Sie angeben wollen, welches Dell OMCI-Gerät zum Auffüllen der Liste der Einstellungen verwendet werden soll, wählen Sie dieses Gerät in der Liste **Alle Geräte** aus.
2. Klicken Sie auf **Konfigurieren > Dell OMCI-Konfiguration**.
3. Um nur diejenigen BIOS-Einstellungen zu übertragen, die Sie in der Liste ändern, wählen Sie **Nur geänderte Einstellungen auf die Zielclients anwenden** aus. Um den gesamten Satz BIOS-Einstellungen auf die Zielgeräte zu übertragen, wählen Sie **Alle Einstellungen auf Zielclients anwenden** aus.
4. Ändern Sie in der Liste der BIOS-Einstellungen die Einstellung für alle Elemente, die geändert werden sollen. Klicken Sie in der Spalte **Neue Einstellung** auf den Pfeil nach unten, um eine Auswahl aus einer Liste von Optionen zu treffen.
5. Um das BIOS-Kennwort zu ändern, wählen Sie **Set the BIOS password** (BIOS-Kennwort festlegen). Geben Sie das neue Kennwort ein und bestätigen Sie es. Um das BIOS-Kennwort zu löschen, müssen Sie beide Kennwortfelder löschen.
6. Um das BIOS-Assetkennzeichen für das Gerät zu ändern, wählen Sie **Set the BIOS asset tag** (BIOS-Assetkennzeichen festlegen) und geben das neue Kennzeichen in das Textfeld **Asset tag** (Assetkennzeichen) ein.

7. Klicken Sie auf **OK**, um die Konfiguration zu speichern.
   Es wird ein Konfigurationspaket mit den Einstellungen erstellt, die Sie geändert haben. Um die Konfiguration auf die von Ihnen verwalteten Dell OMCI-Geräte zu übertragen, müssen Sie einen Zeitplan für die Verteilung des Pakets auf die Zielgeräte definieren.
8. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
9. Wählen Sie das Paket in der Liste **Alle Pakete** aus. Es trägt die Bezeichnung **Dell OMCI BIOS-Einstellungen - <Datum - Uhrzeit>**.
   Sie können das Paket dahingehend umbenennen, dass der Paketname Aufschluss über die Einstellungen gibt, die konfiguriert werden, oder eine Beschreibung bietet, auf welche Geräte die Einstellungen übertragen werden.
10. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Geplanten Task erstellen** aus.
11. Das Paket wird im Extra **Geplante Tasks** angezeigt. Ziehen Sie jedes Dell OMCI-Gerät aus der Netzwerkansicht auf das OMCI-Paket.
12. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Eigenschaften** aus, um die Paketeigenschaften anzuzeigen.
13. Klicken Sie auf **Verteilungsmethode** und wählen Sie **Push** als **Verteilungstyp**. Anschließend wählen Sie **Push-Standardverteilung** als **Verteilungsmethode** aus. Klicken Sie auf **Speichern**.
14. Klicken Sie mit der rechten Maustaste auf das Paket und wählen Sie **Jetzt starten** aus.
    Bei fortschreitendem Verteilungstask ändert sich der Paketstatus. Wenn die Verteilung abgeschlossen ist, zeigt der Status die Anzahl der Geräte an, für die der Verteilungstask erfolgreich durchgeführt wurde bzw. fehlgeschlagen ist.

Nachdem das Paket erfolgreich verteilt wurde, können Sie jedes der von Ihnen neu konfigurierten Geräte neu starten und das BIOS-Setup aufrufen, um die Durchführung der Änderungen zu kontrollieren.

Verwalten von Dell DRAC-Geräten

LANDesk Management Suite umfasst eine Management-Integrationsfunktion für Geräte, die mit einem Dell Remote Access Controller (DRAC) ausgestattet sind. Der DRAC ist ein Remote Hardware-Controller, der als Schnittstelle zur IPMI-fähigen Servermanagement-Hardware auf dem Dell-Gerät dient. Dem DRAC ist eine IP-Adresse zugeordnet, die zur Identifizierung des DRAC bei der Erkennung und Verwaltung des Geräts dient.

Geräte mit Dell DRAC können mit den gleichen Funktionen verwaltet werden wie andere IPMI-fähige Geräte. Wenn das Gerät erkannt und in die Liste der verwalteten Geräte aufgenommen wurde, wird es wie jedes andere IPMI-Gerät verwaltet. Zusätzlich besitzt Management Suite spezielle Dell DRAC-Funktionen.

Der OpenManage Server Administrator ist eine webbasierte Konsole von Dell zur Verwaltung des DRAC-Geräts. Normalerweise erfolgt der Zugriff durch Eingabe der IP-Adresse des DRAC in einen Browser und Anmeldung mit Benutzername und Kennwort. Wenn ein Dell DRAC-Gerät mit Management Suite verwaltet wird, kann dieses Dienstprogramm auch direkt von der Management Suite Schnittstelle aus gestartet werden.

Außerdem ermöglicht Management Suite die Verwaltung von Benutzernamen und Kennwörtern für den Zugriff auf den OpenManager Server Administrator, und es werden drei Protokolle von diesem Dienstprogramm in der Serverinformationskonsole angezeigt.

So öffnen Sie den OpenManage Server Administrator für ein Dell DRAC-Gerät

1. Klicken Sie in der Management Suite Netzwerkansicht auf das Dell DRAC-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Erweitern Sie in der Echtzeitinventar-Konsole die Option **Hardware** und klicken Sie auf **Dell DRAC**. Die IP-Adresse sowie andere Informationen zur Identifizierung des Geräts werden angezeigt.
3. Klicken Sie auf die Schaltfläche **Starten** des **Dell DRAC-Dienstprogramms**, um das DRAC-Dienstprogramm des Geräts zu öffnen, oder klicken Sie auf die Schaltfläche **Starten** für die **Dell DRAC-Energieverwaltung**, um den OpenManage Server Administrator des Geräts in einem neuen Fenster zu öffnen.

In Management Suite verfügbare Dell DRAC-Protokolle

Drei Protokolle vom Dienstprogramm "OpenManage Server Administrator" werden in der Management Suite Echtzeitinventar-Konsole angezeigt.

- **Dell DRAC-Protokoll:** Verfolgt alle vom Server Administrator aufgezeichneten Ereignisse, wie z. B. Anmeldeaktivität, Sitzungsstatus, Firmware-Updatestatus sowie DRAC-Interaktion mit anderen Gerätekomponenten. In Management Suite angezeigte Informationen sind u. a. Schwere des Fehlers, Beschreibung und empfohlene Fehlerbehebungsmaßnahmen.
- **Dell DRAC-Befehlsprotokoll:** Verfolgt alle an den Server Administrator ausgegebenen Befehle. Es wird angegeben, welche Befehle wann und von wem ausgeführt wurden, einschließlich An- und Abmeldeversuche und Zugangsfehler.
- **Dell DRAC-Ablaufverfolgungsprotokoll:** Diese Protokoll ist bei der Ablaufverfolgung der Netzwerkkommunikation hilfreich und bietet Details z. B. zu Alarmierung, Paging oder Netzwerkverbindungen vom DRAC.

So zeigen Sie die Protokolle für ein Dell DRAC-Gerät an

1. Klicken Sie in der Management Suite Netzwerkansicht auf das Dell DRAC-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie in der Echtzeitinventar-Konsole auf **Protokolle**.
3. Klicken Sie auf **Dell DRAC-Protokoll**, **Dell DRAC-Befehlsprotokoll** oder **Dell DRAC-Ablaufverfolgungsprotokoll**.

Verwalten von Benutzernamen für Dell DRAC-fähige Geräte

Um auf die OpenManage Server Administrator-Schnittstelle zuzugreifen, melden Sie sich mit einem für das Gerät definierten Benutzernamen und Kennwort an. Der Standard **root**-Benutzer ist der erste Benutzer in der Liste. Er kann nicht gelöscht, jedoch kann sein Kennwort geändert werden. Es können bis zu 15 zusätzliche Benutzer hinzugefügt werden. DRAC-Benutzernamen können zwar verschiedene Zugangsebenen haben, Management Suite definiert Benutzernamen jedoch nur auf der Administratorebene.

So können Sie Benutzernamen und Kennwörter für ein DRAC-fähiges Gerät hinzufügen oder bearbeiten

1. Klicken Sie in der Management Suite Netzwerkansicht auf das Dell DRAC-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie in der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.

3. Erweitern Sie in der Hardwarekonfigurationskonsole die Option **Dell DRAC-Konfiguration** und klicken Sie auf **Dell DRAC-Benutzer**. Es wird eine Liste der derzeit definierten Benutzer angezeigt.
4. Um das Kennwort zu ändern, klicken Sie auf die Benutzernummer und dann auf **Kennwort ändern**. Nachdem Sie das neue Kennwort eingegeben und bestätigt haben, klicken Sie auf **Übernehmen**. (Um das gleiche Kennwort mehreren Benutzern zuzuweisen, wählen Sie dies mit Strg + Mausklick oder Umschalt + Mausklick aus.)
5. Um einen Benutzer hinzuzufügen, klicken Sie auf **Benutzer hinzufügen**. Geben Sie einen Benutzernamen und ein Kennwort ein, bestätigen Sie das Kennwort und klicken Sie auf **Übernehmen**. Der Benutzer wird zur Liste hinzugefügt.

   Wenn Sie einen Benutzernamen eingeben, der sich bereits in der Liste befindet, überschreibt das neue Kennwort, das Sie eingeben, das alte Kennwort für diesen Benutzernamen. Es wird kein zweiter Benutzer mit dem gleichen Namen zur Liste hinzugefügt.

6. Um einen Benutzer zu löschen, klicken Sie auf die Benutzernummer, auf **Benutzer löschen** und dann auf **OK**. (Um mehrere Benutzer zu löschen, wählen Sie diese mit Strg + Mausklick oder Umschalt + Mausklick aus.)

Alle Benutzer in dieser Liste haben Zugang auf der Administratorebene zum OpenManage Server Administrator.

IPMI-Unterstützung

LANDesk Management Suite unterstützt IPMI (Intelligent Platform Management Interface) 1.5 und 2.0. IPMI ist eine von Intel, Hewlett-Packard, NEC und Dell entwickelte Norm, die die Nachrichten- und Systemschnittstelle für verwaltbare Hardwarebestandteile definiert. IPMI enthält Überwachungs- und Wiederherstellungsfunktionen, mit denen Sie auf zahlreiche Funktionen zugreifen können, unabhängig davon, ob der Rechner eingeschaltet ist oder in welchem Zustand sich das Betriebssystem befindet. Weitere Details zu IPMI erhalten Sie auf Intels Website.

Die IPMI-Überwachung wird vom Baseboard Management Controller (BMC) verwaltet. BMC läuft mit Standbystrom und ruft selbstständig Daten zum Systemzustand ab. Sie können die Gegenmaßnahmen konfigurieren, die von IPMI eingeleitet werden, wenn BMC erkennt, dass die Werte eines Elements außerhalb des gültigen Bereichs liegen. Zu diesen Maßnahmen gehört beispielsweise das Aufzeichnen des Ereignisses in einem Protokoll, das Erstellen von Warnmeldungen oder Ausführen automatischer Wiederherstellungsaktionen (System herunterfahren oder zurücksetzen usw.).

Damit BMC auf dem System erkannt wird, muss SMBIOS 2.3.1 oder höher installiert sein. Wird BMC nicht erkannt, sehen Sie möglicherweise keine IPMI-Informationen in Berichten, Exportvorgängen usw.

IPMI definiert Schnittstellen für Hardwarebestandteile, die zur Überwachung von Kontrollsignalen für den Systemzustand verwendet werden (beispielsweise Temperatur, Versorgungsspannung, Lüfter, Stromzufuhr und unbefugtes Öffnen von Gehäusen). Neben den Leistungen zur Überwachung des Systemzustands bietet IPMI Systemverwaltungsfunktionen wie automatische Warnmeldungen, automatisches Herunterfahren und Neustarten des Systems, remotegesteuerter Neustart und Energieverwaltungslösungen sowie Assetverfolgung.

Was die Optionen im Management Suite-Menü betrifft, gibt es für IPMI-kompatible Geräte je nach Betriebssystemzustand geringfügige Unterschiede zu beachten.

Verwaltungsfunktionen für IPMI-kompatible Geräte

Welche Überwachungsfunktionen unterstützt werden, hängt davon ab, welche Komponenten auf dem überwachten Gerät installiert wurden und in welchem Zustand sich das Gerät befindet. Jedes IPMI-aktivierte Gerät, das über einen Baseboard Management Controller (BMC) verfügt, kann von der Verwaltungskonsole in begrenztem Umfang ohne zusätzliche Verwaltungsagenten überwacht werden, nachdem der BMC konfiguriert wurde. Dies schließt die Out-of-Band-Verwaltung ein, wenn das Gerät heruntergefahren wird oder das Betriebssystem nicht funktionsfähig ist.

Das komplette Spektrum an Verwaltungsfunktionen ist verfügbar, wenn folgende Bedingungen erfüllt sind: Der LANDesk Management Agent ist installiert, ein BMC ist vorhanden, das Gerät ist eingeschaltet und das Betriebssystem ist funktionsfähig. Die folgende Tabelle vergleicht die verfügbare Funktionalität in unterschiedlichen Konfigurationen.

	Nur BMC*	BMC + Agent	Agent (kein IPMI)
Für Out-of-Band-Verwaltung konfiguriert	X	X	
Für In-Band-Verwaltung konfiguriert		X	X
Gerät wird erkannt**	X	X	X
Umgebungssensoren lesen	X	X	Hard-wareabhängig
Remotes Ein-/Ausschalten	X	X	X
Ereignisprotokoll lesen & löschen	X	X	
Alarmmeldungen konfigurieren	X	X	X
Betriebssysteminformationen lesen		X	X
Ordnungsgemäßes Herunterfahren		X	X
SMBIOS-Informationen lesen (Prozessor, Einschübe, Speicher)		X	X
IP-Synchronisierung (Betriebssystem nach BMC)		X	

	Nur BMC*	BMC + Agent	Agent (kein IPMI)
Watchdog-Timer		X	
BMC kommuniziert mit Coreserver	X	X	
Lokale Management Suite Komponenten kommunizieren mit dem Coreserver		X	X
Komplettes Spektrum von Management Suite Verwaltungsfunktionen		X	

*Standard BMC. Mini-BMC ist eine abgespeckte Version eines Baseboard Management Controllers. Es verfügt über die oben aufgeführten Funktionen mit Einschränkungen in den folgenden Bereichen:

- Unterstützt keine SOL-Umleitung (Serial over LAN)
- Besitzt nur einen Benutzernamen für BMC Management
- Verwendet nur einen Kanal für die Kommunikation mit dem BMC
- Verfügt über einen kleineren System Event Log (SEL)-Pool

**Wenn der BMC nicht konfiguriert ist, reagiert er nicht auf ASF-Pings; diese Pings werden vom Produkt für die IPMI-Erkennung verwendet. Das heißt, dass Sie das Produkt als normalen Computer erkennen lassen müssen. Beim Bereitstellen eines Verwaltungsagenten durchsucht die ausführbare Datei der Serverkonfiguration das System, erkennt es als IPMI und konfiguriert den BMC.

Konflikte mit IPMI-Treibern

Wenn Sie dieses Produkt auf einem IPMI-Gerät installieren und auf dem Gerät bereits ein hardwarespezifischer IPMI-Treiber installiert ist, dann verwendet dieses Produkt den Treiber, falls er davon unterstützt wird.

Wenn kein IPMI-Treiber auf dem Gerät installiert ist, installiert Management Suite den OSA IPMI-Treiber.

Wenn Sie andere Verwaltungslösungen mit integrierten IPMI-Treibern auf Geräten installiert haben, die Sie mit diesem Produkt verwalten möchten, müssen Sie wahrscheinlich diese Produkte deinstallieren, bevor Sie Management Suite Agenten mit IPMI-Verwaltungsfunktionen bereitstellen können.

Beispiel: Microsoft Windows Server 2003 umfasst IPMI-Support über die Installation von Windows Remote Management (WinRM), wobei WinRM einen Windows Management Instrumentation (WMI)-Provider und einen IPMI-Treiber enthält. Management Suite unterstützt jedoch die Installation dieses IPMI-Treibers nicht und installiert einen eigenen IPMI-Treiber. Wenn WinRM auf einem Gerät installiert ist, das Sie mit Management Suite verwalten möchten, müssen Sie zunächst WinRM über Windows Programme hinzufügen/entfernen deinstallieren.

IPMI BMC-Konfiguration

Die Seite **IPMI BMC-Konfiguration** verwenden Sie, um die Einstellungen für die Kommunikation mit IPMI-tauglichen Geräten anzupassen. Die unten beschriebenen Funktionen stehen für In-Band-Geräte zur Verfügung; bei Out-of-Band-Geräten stehen nur die Stromkonfiguration und die BMC-Benutzereinstellungen zur Verfügung.

VORSICHT: Es wird dringend davon abgeraten, IPMI-Einstellungen zu ändern, es sei denn, Sie sind mit der IPMI-Spezifikation vertraut und kennen die mit diesen Einstellungen verknüpften Technologien. Die unsachgemäße Verwendung dieser Konfigurationsoptionen kann dazu führen, dass Management Suite nicht wie erwartet mit den IPMI-kompatiblen Geräten kommuniziert.

Die folgenden Konfigurationsoptionen stehen zur Verfügung:

- "Ändern der Einstellungen für den Watchdog-Timer" auf Seite 871
- "Ändern der Einstellungen für die Stromkonfiguration" auf Seite 872
- "Ändern von BMC-Benutzereinstellungen" auf Seite 872
- "Ändern des BMC-Kennworts" auf Seite 873
- "Ändern der LAN-Konfigurationen" auf Seite 873
- "Ändern der Serial Over LAN (SOL)-Konfigurationen" auf Seite 875
- "Ändern von IMM-Konfigurationen" auf Seite 875

Ändern der Einstellungen für den Watchdog-Timer

IPMI stellt eine Schnittstelle für den BMC-Watchdog-Timer bereit. Dieser Zeitgeber (Timer) kann so eingestellt werden, dass er regelmäßig abläuft und er ist so konfiguriert, dass er bestimmte Aktionen (z. B. Energiezyklus) initiiert, wenn er abläuft. Management Suite setzt den Zeitgeber in regelmäßigen Abständen zurück, damit er nicht abläuft. Wenn das Gerät nicht mehr zur Verfügung steht (z. B. wenn es heruntergefahren wird oder sich aufhängt), wird der Zeitgeber nicht zurückgesetzt und läuft ab, sodass daraufhin die Aktion initiiert wird.

Sie können angeben, wie viel Zeit verstreichen darf, bevor der Timer abläuft, und Sie können eine Aktion auswählen, die ausgeführt wird, wenn er abläuft. Sie können entweder auf die Ausführung einer Aktion verzichten, einen Kaltstart ausführen (Gerät herunterfahren und neu starten), das Gerät ordnungsgemäß herunterfahren oder einen Energiezyklus ausführen (das Gerät ordnungsgemäß herunterfahren und dann erneut starten).

Sie können den BMC auch so konfigurieren, dass keine weitere ARP (Address Resolution Protocol)-Meldungen gesendet werden, während der Watchdog-Timer aktiviert ist. Hiermit kann das Aufkommen an Netzwerkdaten reduziert werden. Wenn Sie die ARPs einstellen, werden diese automatisch fortgesetzt, wenn der Watchdog-Timer abläuft.

So ändern Sie die Einstellungen für den Watchdog-Timer

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Watchdog-Timer**.
4. Wählen Sie **Watchdog-Timer starten**, um den Zeitgeber zu aktivieren.

5. Geben Sie an, wie oft der Timer überprüft werden soll (Anzahl von Minuten oder Sekunden).
6. Wählen Sie eine Aktion aus, die initiiert wird, sobald der Timer abläuft.
7. Wenn Sie BMC am Senden weiterer ARP-Meldungen hindern möchten (während der Watchdog-Timer aktiviert ist), wählen Sie **BMC ARPs aufheben** aus.
8. Klicken Sie auf **Übernehmen**.
9. Wenn Sie die Einstellungen für den Watchdog-Timer geändert haben, können Sie die Standardeinstellungen wiederherstellen, indem Sie auf **Standardeinstellungen wiederherstellen** klicken.

Ändern der Einstellungen für die Stromkonfiguration

Wenn es auf einem IPMI-kompatiblen Computer zu einem Stromausfall kommt, können Sie festlegen, welche Maßnahme beim Wiederherstellen der Stromzufuhr ergriffen werden sollen. Es wird empfohlen, den Computer in dem Zustand wiederherzustellen, in dem er sich zum Zeitpunkt des Stromausfalls befand. Sie können jedoch auch festlegen, dass der Computer ausgeschaltet bleiben soll oder immer hochgefahren werden soll.

So ändern Sie die Einstellungen für die Stromkonfiguration

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Stromkonfiguration**.
4. Wählen Sie eine Option aus, die beim Wiederherstellen der Stromzufuhr aktiviert werden soll.
5. Klicken Sie auf **Übernehmen**.
6. Wenn Sie die Einstellungen für die Stromkonfiguration geändert haben, können Sie die Standardeinstellungen wiederherstellen, indem Sie auf **Standardeinstellungen wiederherstellen** klicken.

Ändern von BMC-Benutzereinstellungen

Management Suite authentifiziert sich gegenüber einem BMC mit einer für den BMC eindeutigen Benutzername/Kennwort-Kombination (separat von allen anderen Management Suite Benutzernamen). Management Suite reserviert den ersten Benutzernamen, damit er immer mit dem BMC kommunizieren kann. Wenn der BMC das Definieren anderer Benutzernamen unterstützt, können Sie Benutzernamen mit Kennwörtern für die BMC-Authentifizierung definieren.

Sie können auch Berechtigungsebenen für die einzelnen Benutzer angeben. Für erweiterte IMMs können Sie pro Kanal Protokoll-Berechtigungsebenen angeben (telnet, http und https).

VORSICHT: Gehen Sie äußerst umsichtig vor, wenn Sie diese Einstellungen ändern. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

So ändern Sie BMC-Benutzereinstellungen

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Benutzereinstellungen**.

4. Um die Daten für einen Benutzernamen zu löschen, klicken Sie auf die Indexzahl und dann auf **Löschen**.
5. Klicken Sie zum Hinzufügen oder Ändern eines Benutzernamens auf die Indexzahl und dann auf **Bearbeiten**. Geben Sie einen Benutzernamen ein.
7. Um ein Kennwort festzulegen, aktivieren Sie das Kontrollkästchen **Kennwort festlegen**, geben dann das Kennwort ein und bestätigen es.
8. Wählen Sie die Berechtigungsebenen für LAN-Zugriff und seriellen Zugriff aus.
9. Klicken Sie auf **Änderungen speichern**.

Ändern des BMC-Kennworts

Management Suite authentifiziert sich gegenüber dem BMC eines Geräts mithilfe des Standardbenutzernamens (Benutzer 1 und Kennwort). Der Benutzername kann nicht geändert werden, sondern nur das Kennwort. Wenn Sie diese Kennworteinstellung ändern, wird die Änderung in der Datenbank auf dem BMC gespeichert.

So ändern Sie das BMC-Standardkennwort

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **Kennwort**.
4. Geben Sie das neue Kennwort ein und bestätigen Sie es.
5. Klicken Sie auf **Übernehmen**.

Ändern der LAN-Konfigurationen

IPMI-Meldungen können direkt vom BMC über eine LAN-Schnittstelle (zusätzlich zur Systemschnittstelle des Geräts) übermittelt werden. Das Aktivieren der LAN-Kommunikation ermöglicht es dem Coreserver, IPMI-spezifische Warnungen zu empfangen, selbst wenn das Gerät heruntergefahren wurde. Der Coreserver hält diese Kommunikationsverbindung aufrecht, solange das Gerät über eine physikalische Netzwerkverbindung mit einer gültigen Netzwerkadresse verfügt, und solange die Hauptstromzufuhr des Geräts eingeschaltet bleibt.

VORSICHT: Wenn Sie eine benutzerdefinierte Konfiguration für die LAN- oder serielle Kommunikation auf den BMC festlegen, sollten Sie beim Ändern der Einstellungen mit äußerster Vorsicht vorgehen. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

Wenn Sie über einen definierten LAN-Kanal verfügen, können Sie die Standardeinstellungen für den BMC des Geräts verwenden oder die Einstellungen für IP-Adresse und Gateway ändern. Verwenden Sie diese Optionen, um Ziele für die SNMP-Traps zu konfigurieren, die vom BMC für jede Plattformereignis-Trap (PET, Platform Event Trap) gesendet werden.

Sie können auch die Einstellungen für das Senden von Alarmen über LAN in den Einstellungen für die SNMP-Community-Zeichenfolge ändern. Beim Konfigurieren dieser Einstellungen müssen Sie den für die SNMP-Authentifizierung verwendeten SNMP-Community-Zeichenfolge angeben. Sie können für jede Konfiguration die Informationen zum Trap-Ziel bearbeiten, um anzugeben, wo und wie Traps gesendet und ob sie bestätigt werden.

So legen Sie Eigenschaften für die LAN-Channel-Konfiguration fest

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **LAN-Konfiguration**.
4. Wählen Sie in der Liste "LAN-Kommunikation" die Option **Immer verfügbar** aus, um den Zugriff auf den BMC offen zu halten. Wenn Sie **Deaktiviert** auswählen, haben Sie keinen LAN-Zugriff auf den BMC, wenn das Gerät out-of-band ist.
5. Wählen Sie die **Benutzerberechtigungsebene** für den Kanal aus: Die Ebene **Administratorrechte** hat Zugriff auf alle Befehle, wohingegen die **Benutzer-Ebene** auf schreibgeschützten Zugriff beschränkt ist. Wenn Sie **Benutzer-Ebene** wählen, steht Ihnen nur eine eingeschränkte Auswahl von Funktionen zur Verfügung.
6. Wählen Sie **BMC ARPs dauerhaft deaktivieren**, um die vom BMC ausgehenden Address Resolution Protocol-Meldungen auszuschalten. Damit wird zwar das Aufkommen an Netzwerkdaten reduziert, jedoch möglicherweise auch die Kommunikation mit dem BMC verhindert, wenn das Gerät out-of-band ist.
7. Wählen Sie **ARP-Antworten ausschalten**, um den BMC am Senden von ARP-Meldungen zu hindern, wenn das Betriebssystem nicht verfügbar ist. Wenn Sie diese Einstellung aktivieren, verhindern Sie möglicherweise die Kommunikation mit dem BMC, wenn das Gerät out-of-band ist.
8. IP-Einstellungen für den LAN-Kanal werden automatisch festgelegt, wenn der BMC mit dem Betriebssystemkanal synchronisiert ist. Falls nicht, ist das Kontrollkästchen der Registerkarte **IP-Einstellungen** aktiviert. Sie können die Aktivierung des Kontrollkästchens beibehalten, um automatisch bereitgestellte DHCP-Einstellungen zu verwenden; oder Sie können das Kontrollkästchen deaktivieren und die Textfelder mit statischen Einstellungen bearbeiten. Im Allgemeinen ist der Verwendung der automatischen Einstellungen der Vorzug zu geben.
9. Klicken Sie auf die Registerkarte **Alarme über LAN senden**, um die Einstellungen für die SNMP-Community-Zeichenfolge zu konfigurieren (siehe die Schritte weiter unten).
10. Klicken Sie auf **Übernehmen**, um Ihre Änderungen zu speichern.

HINWEIS: Wenn Sie auf die Schaltfläche **Standardeinstellungen wiederherstellen** auf dieser Seite klicken, werden die Einstellungen unter der Überschrift **Eigenschaften für LAN-Kanal** auf ihre Standardwerte zurückgesetzt, andere Einstellungen auf der Seite bleiben jedoch unverändert. Wenn Sie Daten auf der Registerkarte **IP-Einstellungen** ändern und auf **Übernehmen** klicken, müssen Sie diese Einstellungen manuell zurücksetzen.

So ändern Sie die Einstellungen für "Alarme über LAN senden"

1. Öffnen Sie die Seite **LAN-Konfiguration** (Schritte 1-3 oben).
2. Klicken Sie auf die Registerkarte **Alarme über LAN senden**.
3. Aktivieren Sie das Kontrollkästchen **Aktiviert**, um das Senden von SNMP-Alarmen zu ermöglichen.
4. Geben Sie den für die SNMP-Authentifizierung zu verwendenden **SNMP-Community-Zeichenfolge** an.
5. Doppelklicken Sie zum Konfigurieren der Trap-Ziele auf die Indexzahl, um das Dialogfeld **Eigenschaften** zu öffnen.

6. Wählen Sie **Dieses Warnmeldungsziel aktivieren** aus. Geben Sie die IP-Adresse an, an die der BMC Alarmmeldungen senden wird, und geben Sie die entsprechende MAC-Adresse an.
7. Geben Sie die Anzahl der Wiederholungsversuche, die Häufigkeit der Wiederholungen und das bevorzugt zu verwendende Gateway an.
8. Wenn Sie veranlassen möchten, dass die Alarmmeldungen bestätigt werden (verursacht ein erhöhtes Aufkommen an Netzwerkdaten), aktivieren Sie das Kontrollkästchen **Alarm bestätigen**.
9. Klicken Sie auf **OK**.
10. Klicken Sie auf der Seite "LAN-Konfiguration" auf **Übernehmen**, nachdem alle Einstellungen vollständig angegeben wurden.

Ändern der Serial Over LAN (SOL)-Konfigurationen

Verwenden Sie SOL (Serial Over LAN), um serielle Modemeinstellungen für bestimmte Verwendungszwecke anzupassen, beispielsweise das Umleiten von BIOS POST-Nachrichten an den seriellen Anschluss. Wenn der BMC über eine Modemverbindung nach außen wählen muss, müssen außerdem spezifische Modemeinstellungen wie Initialisierungs- und Wählzeichenfolgen angegeben werden.

Für seriellen Modembetrieb müssen Sie möglicherweise die BIOS- und Jumper-Einstellungen der Geräteplatine konfigurieren. Weitere Informationen finden Sie in der Dokumentation des entsprechenden Geräts.

VORSICHT: Wenn Sie die benutzerdefinierte Konfiguration für die LAN- oder serielle Kommunikation auf den BMC festlegen, sollten Sie beim Ändern der Einstellungen mit äußerster Vorsicht vorgehen. Falsche Einstellungen können die BMC-Kommunikation des Geräts mit diesem Produkt deaktivieren.

So ändern Sie die SOL-Konfigurationseinstellungen

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.
2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **SOL-Konfiguration**.
4. Aktivieren Sie **Serial-Over-LAN-Kommunikationen einschalten**, um SOL zu aktivieren.
5. Wählen Sie **Benutzerebene erforderlich, um SOL zu aktivieren** zum Festlegen der mindestens erforderlichen Benutzerebene.
6. Wählen Sie die **Baudrate für SOL-Sitzungen**, die zur Hardwarekonfiguration des Geräts passt.
7. Klicken Sie auf **Übernehmen**.

Ändern von IMM-Konfigurationen

Die Seite **IMM-Konfiguration** wird nur für IPMI-Geräte angezeigt, die über eine erweiterte IMM Add-in-Karte verfügen. Mit den Optionen auf dieser Seite können Sie Protokolle und Funktionen zur Verwendung mit dem IMM-tauglichen Gerät aktivieren oder deaktivieren. Konsultieren Sie die Dokumentation des IMM-Herstellers, bevor Sie diese Einstellungen ändern.

So ändern Sie IMM-Konfigurationseinstellungen

1. Klicken Sie in der Management Suite Netzwerkansicht mit der rechten Maustaste auf das IPMI-Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.

2. Klicken Sie im linken Navigationsfenster der Echtzeitinventar-Konsole auf **Hardwarekonfiguration**.
3. Erweitern Sie **IPMI BMC-Konfiguration** und klicken Sie auf **IMM-Konfiguration**.
4. Markieren Sie die Kontrollkästchen für Protokolle und Funktionen, die Sie aktivieren möchten, und fügen Sie alle etwaigen erforderlichen Einstellungen hinzu.

   Verfügbare Optionen sind: KVM, SNMP, telnet, SMTP-Alarmierung, HTTP und HTTPS.

5. Klicken Sie auf **Übernehmen**.

Intel vPro

Konfigurieren von Intel vPro-Geräten

Geräte mit Intel vPro-Funktionalität sollten beim ersten Einrichten und Hochfahren konfiguriert (oder "versorgt") werden, um die Intel vPro-Funktionen zu aktivieren. In diesen Vorgang sind mehrere Sicherheitsvorkehrungen eingebettet, die gewährleisten, dass nur berechtigte Benutzer Zugang zu den Intel vPro-Verwaltungsfunktionen erhalten.

Intel vPro-Geräte kommunizieren mit einem Versorgungsserver auf dem Netzwerk. Der Versorgungsserver wartet auf Meldungen von Intel vPro-Geräten in Netzwerk und ermöglicht dem IT-Personal die Verwaltung von Servern über Out-of-Band-Kommunikation, unabhängig vom Status des Betriebssystems des jeweiligen Geräts. Der Coreserver agiert als Versorgungsserver für Intel vPro-Geräte und umfasst Funktionen, die Sie bei der Versorgung von Geräten im Rahmen der Einrichtung unterstützen. Sie können die Geräte dann mit oder ohne zusätzliche Verwaltungsagenten verwalten.

Intel vPro-Versorgungsoptionen

Grundsätzlich gibt es drei Möglichkeiten für die Versorgung von Intel vPro-Geräten. Welche Versorgungsmethode Sie verwenden, hängt von der AMT-Versionsnummer der von Ihnen verwalteten Geräte und auch von Ihren Präferenzen ab. Informationen zu den verschiedenen Versorgungsmethoden finden Sie in weiteren Hilfethemen, wie unten angegeben.

One-Touch-Versorgung (Verwenden von Versorgungskennungen)

Bei der One-Touch-Versorgung können Sie Management Suite verwenden, um einen Satz Versorgungskennungen (PID und PPS) zu erzeugen. Diese Kennungen werden in das Geräte-BIOS eingegeben, um eine sichere Verbindung mit dem Versorgungsserver während des Vorgangs der Erstversorgung zu gewährleisten. Dieses One-Touch-Verfahren kann zur Konfiguration von Geräten der Versionen 2.0 und höher verwendet werden.

Weitere Informationen finden Sie unter "Verwenden von Versorgungskennungen (One-Touch-Versorgung)" auf Seite 881.

Zero-Touch-Versorgung (remote Konfiguration mit Zertifikaten)

Geräte der Versionen 2.2/2.6 und höher können auch unter Verwendung der Remotekonfiguration (auch als "Zero-Touch"-Versorgung bezeichnet) konfiguriert werden. Dieser Prozess erfordert keine Übertragung von PID/PPS-Kennungen, sondern wird automatisch initiiert, nachdem der Versorgungsserver (Coreserver) das Grußpaket des Geräts empfängt oder nachdem ein LANDesk Verwaltungsagent auf dem Intel vPro-Gerät bereitgestellt wurde. Auf dem Coreserver muss ein Intel Clientsetup-Zertifikat von einem autorisierten Zertifikatanbieter installiert sein, damit Sie die Remotekonfiguration verwenden können.

Auf Geräten mit Intel vPro 3.0 und höher wird auch eine "Bare-Metal-" oder agentenlose Remotekonfiguration unterstützt.

Weitere Informationen finden Sie unter "Verwenden der Remoteversorgung (Zero-Touch-Versorgung)" auf Seite 887

Automatische Versorgung für Intel vPro 6.2 und höher

Intel vPro-Geräte mit AMT-Version 6.2 oder höher werden von Management Suite automatisch versorgt. Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben, aber keine PID auf den Geräten festgelegt wurde bzw. kein Zero-Touch-Zertifikat bereitgestellt wurde, werden Ihre Geräte unter Verwendung des Clientsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in gewisser Hinsicht ein und spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen des Gerätesetups erforderlich ist.

Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben und entweder eine PID auf den Geräten festgelegt oder ein Zero-Touch-Zertifikat bereitgestellt haben, werden die Geräte unter Verwendung des Adminsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in keinerlei Weise ein und spiegelt den höheren Grad an Vertrauenswürdigkeit wider, der mit dem Gerätesetup einhergeht.

Weitere Informationen finden Sie unter "Hostgestützte Versorgung" auf Seite 889.

HINWEIS: Beachten Sie, dass die Informationen in diesem Abschnitt allgemeine Beschreibungen der Intel vPro-Konfiguration sind. Die einzelnen Hersteller setzen die Intel vPro-Funktionalität jedoch auf verschiedene Weise ein und es kann in Bereichen wie dem Zugang auf den Intel AMT-oder ME BIOS-Bildschirm, dem Zurücksetzen des Geräts auf Werksmodus (Aufhebung der Versorgung) oder in der Art und Weise, wie PID/PPS-Schlüssel bereitgestellt werden, Unterschiede geben. Sehen Sie sich die vom Gerätehersteller mitgelieferten Unterlagen und Supportinformationen an, bevor Sie mit der Konfiguration beginnen.

Verwendung statischer IP-Adressen bei Intel vPro-Geräten

Auf Intel vPro-Geräten wird zwei Komponenten eine IP-Adresse zugewiesen: dem Intel vPro-Chip und dem Betriebssystem des Geräts. Aus diesem Grund kann es passieren, dass in Ihrer Liste der erkannten Geräte zwei Einträge für dasselbe Intel vPro-Gerät angezeigt werden. Dies geschieht nur, wenn Sie eine statische IP-Adresse anstelle von DHCP verwenden möchten.

Bei Verwendung statischer IP-Adressen für Intel vPro-Geräte sollte die Intel vPro-Firmware mit einer eigenen MAC-Adresse konfiguriert werden. (Wenden Sie sich an Intel, wenn Sie beim Neuinstallieren und ordnungsgemäßen Konfigurieren der Firmware Unterstützung benötigen.)

Nach Abschluss der Konfiguration verfügt das Intel vPro-Gerät über eine andere MAC-Adresse, IP-Adresse und einen anderen Hostnamen als das Betriebssystem des Geräts. Um Intel vPro-Geräte ordnungsgemäß verwalten zu können, müssen für DHCP- und statische IP-Adressen folgende Einstellungen verwenden:

- **DHCP**: Sowohl das Betriebssystem als auch Intel vPro verwenden DHCP und die Hostnamen sind gleich.
- **Statische IP**: Sowohl das Betriebssystem als auch Intel vPro verwenden statische Adressen, die jedoch nicht identisch sind; zudem sind die MAC-Adressen und Hostnamen ebenfalls verschieden.

Wenn ein Intel vPro 2.x-Computer im Enterprise-Modus versorgt wird, kann nur über ein "Hello"-Paket, das an den Setup- und Konfigurationsserver gesendet wird, mit diesem Computer kommuniziert werden. Sobald der Computer von LANDesk Software verwaltet wird, können darauf wie gewöhnlich Intel vPro-Vorgänge ausgeführt werden. Sie sollten nicht versuchen, die IP-Adresse des Betriebssystems zu ermitteln und zu verwalten, da dies dazu führen kann, dass zwei Computereinträge denselben Computer repräsentieren. Da die einzige gemeinsame Kennung zwischen den beiden Geräten die AMT GUID ist und sich die AMT GUID nicht per Remoteverbindung für das Betriebssystemgerät ermitteln lässt, können die beiden Einträge nicht zusammengeführt werden.

Wenn Sie die LANDesk Agenten installieren möchten, können Sie die Agentenkonfiguration nicht per Push vornehmen, da die Intel vPro IP-Adresse die einzige IP-Adresse in der Datenbank ist und das Push-Modul Zugriff auf das Betriebssystem benötigt. Stattdessen müssen die Agenten per Pull (vom verwalteten Intel vPro-Gerät) abgerufen werden. Hierzu ordnen Sie der Freigabe, auf der ein eigenständiges Clientinstallationspaket gespeichert ist, ein Laufwerk zu und führen die ausführbare Datei für die Agentenkonfiguration aus.

Bevor Sie die Agenten abrufen, sollten Sie eine Einstellung im Dienstprogramm "Dienste konfigurieren" ändern, die den Coreserver im Rahmen der Geräteidentifizierung dazu zwingt, die AMT-GUID zu suchen.

So verwenden Sie die AMT-GUID als Identitätsattribut

1. Klicken Sie auf **Start > Alle Programme > LANDesk > LANDesk - Dienste konfigurieren**.
2. Klicken Sie auf der Registerkarte **Inventar** auf **Gerätekennungen**, um doppelt vorhandene Datensätze zu verwalten.
3. Blenden Sie in der **Attributliste** die **AMT-Informationen** ein.
4. Führen Sie einen Bildlauf nach unten durch und verschieben Sie das Attribut **AMT-GUID** in die Liste **Identitätsattribute**.

   Damit wird die AMT-GUID als eines der Attribute erzwungen, die einen Computer eindeutig identifizieren können.

Nachdem Sie diese Einstellung geändert haben, gleicht der Inventardienst die Intel AMT-GUID des Geräts, das sich bereits in der Datenbank befindet, mit den Betriebssysteminformationen in der Scandatei ab (der Vorgang wird beim Importieren des Inventarscans aus dem verwalteten Intel vPro-Gerät in die Datenbank ausgeführt).

Ändern des Kennworts für Intel vPro-Geräte

Zur Kommunikation mit und für die Versorgung von neuen Intel vPro-Geräten ist ein sicheres Kennwort erforderlich. Für Geräte, die Sie verwalten werden, sollte das "Admin"-Kennwort, das Sie auf dem Intel AMT-Konfigurationsbildschirm eingeben (der über das Geräte-BIOS angezeigt wird) mit dem Kennwort übereinstimmen, das Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" eingegeben haben. Dieses Kennwort wird in der Management Suite Datenbank gespeichert und global bei der Versorgung von Intel vPro-Geräten angewendet.

Die sichere Kommunikation bei Intel vPro erfordert sichere Kennwörter. Kennwörter sollten folgende Anforderungen erfüllen:

- Mindestens 8 Zeichen lang
- Mindestens eine Zahl (0 bis 9)

- Mindestens ein nicht alphanumerisches ASCII-Zeichen (z. B. !, &, %)
- Lateinische Groß- und Kleinbuchstaben oder Nicht-ASCII-Zeichen (UTF+00800 und höher).

Nach der Versorgung der Geräte sollten Sie die Kennwörter als Teil Ihres IT-Wartungsplans regelmäßig ändern. Sie können für jedes Intel vPro-Gerät ein anderes Kennwort oder ein neues Kennwort für mehrere Geräte verwenden. Die von Ihnen eingegebenen neuen Kennwörter werden in der Datenbank gespeichert und von Management Suite für die sichere Kommunikation mit verwalteten Intel AMT-Geräten verwendet.

Hostgestützte Versorgung für Intel vPro 6.2 und höher

Management Suite verwendet hostgestützte Versorgung von Intel vPro-Geräten mit AMT-Version 6.2 oder höher. Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben, aber keine PID (One-Touch-Provisioning) auf den Geräten festgelegt wurde bzw. kein Zero-Touch-Zertifikat bereitgestellt wurde, werden Ihre Geräte unter Verwendung des Clientsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in gewisser Hinsicht ein und spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen des Gerätesetups erforderlich ist.

Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben und entweder eine PID auf den Geräten festgelegt oder ein Zero-Touch-Zertifikat bereitgestellt haben, werden die Geräte unter Verwendung des Adminsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in keinerlei Weise ein und spiegelt den höheren Grad an Vertrauenswürdigkeit wider, der mit dem Gerätesetup einhergeht.

Ändern des Intel vPro-Kennworts

So ändern Sie das Kennwort für alle Intel vPro-Geräte

1. Klicken Sie beim Coreserver auf **Konfigurieren > Intel vPro-Optionen > Allgemeine Konfiguration**.
2. Geben Sie unter **Setup und Konfiguration** ein sicheres Kennwort ein und bestätigen Sie das Kennwort.
3. Um das Kennwort auf alle derzeit verwalteten Intel vPro-Geräte anzuwenden, markieren Sie das Kontrollkästchen **Dieses Kennwort synchronisieren**.
4. Wenn Sie eine hochsichere Konfigurationsumgebung besitzen und es vorziehen, den TLS-Modus nicht bei der Konfiguration neuer Geräte zu verwenden, markieren Sie das Kontrollkästchen **Non-TLS-Kommunikation verwenden**. Diese Option wird aufgrund der Sicherheitsrisiken, die die Verwendung eines weniger sicheren Kommunikationsverfahrens mit sich bringen kann, nicht empfohlen.
5. Klicken Sie auf **OK**.

Diese Änderung wird vorgenommen, wenn die Clientkonfiguration ausgeführt wird.

So ändern Sie das Kennwort für ein Intel vPro-Gerät

1. Klicken Sie in der Liste **Alle Geräte** mit der rechten Maustaste auf ein verwaltetes Intel vPro-Gerät und wählen Sie **Intel vPro Kennwort ändern** aus.
2. Geben Sie das neue Kennwort ein und bestätigen Sie es.
3. Klicken Sie auf **OK**.

Verwenden von Versorgungskennungen (One-Touch-Versorgung)

Intel vPro-Geräte kommunizieren mit einem Versorgungsserver auf dem Netzwerk. Der Versorgungsserver wartet auf Meldungen von Intel vPro-Geräten und ermöglicht dem IT-Personal die Verwaltung von Servern über Out-of-Band-Kommunikation, unabhängig vom Status des Betriebssystems des jeweiligen Geräts. Der Coreserver agiert als Versorgungsserver für Intel vPro-Geräte und umfasst Funktionen, die Sie bei der Versorgung von Geräten im Rahmen der Einrichtung unterstützen.

Generieren Sie für jedes Intel vPro-Gerät, das Sie versorgen möchten, eine Versorgungskennung (PID) und eine Versorgungs-Passphrase (PPS). Eine PID (Provisioning ID) ist eine 8 Zeichen umfassende verschlüsselte Kennung, mit der sichergestellt wird, dass der Benutzer über die Berechtigung zur Konfiguration eines Intel vPro-Geräts verfügt. Eine PPS (Provisioning Passphrase) ist ein 32 Zeichen umfassendes Kennwort zur Authentifizierung der PID. Die PID und die PPS werden gegeneinander abgestimmt.

Prozess für die Verwendung von Intel vPro-Versorgungskennungen

Dieser Abschnitt beschreibt den Vorgang der One-Touch-Versorgung für Intel vPro 2.0 und höher.

Wenn ein Intel vPro-Gerät geliefert wird, ist es Aufgabe des IT-Technikers, den Computer zusammenzusetzen und einzuschalten. Nach dem Einschalten des Geräts meldet sich der Techniker im BIOS-basierten Intel ME-Konfigurationsbildschirm (Management Engine) an und ändert das Standardkennwort (admin) in ein starkes Kennwort. Dies ermöglicht den Zugriff auf den Intel AMT-Konfigurationsbildschirm.

Im Intel AMT-Konfigurationsbildschirm werden folgende Informationen für die Versorgung eingegeben:

- eine Versorgungskennung (PID = Provisioning ID)
- ein vor der Versorgung zu verwendender "PPS"-Schlüssel (auch als Preshared Key oder PSK bezeichnet)
- die IP-Adresse des Versorgungsservers
- Port 9971 zur Kommunikation mit dem Versorgungsserver
- der Enterprise-Modus sollte ausgewählt sein
- der Hostname des Intel vPro-Geräts

Der PPS wird zwar vom Versorgungsserver und von dem verwalteten Gerät gemeinsam genutzt, darf jedoch aus Sicherheitsgründen nicht über das Netzwerk übertragen werden. Er muss manuell am Gerät eingegeben werden (im Intel AMT-Konfigurationsbildschirm). Management Suite erzeugt PID/PPS-Paare und speichert diese in der Datenbank. Sie können eine Liste mit generierten Kennungspaaren zur Verwendung bei der Versorgung drucken, oder Sie können die Kennungspaare in eine Schlüsseldatei auf ein USB-Laufwerk exportieren.

Der IT-Techniker sollte die IP-Adresse des Management Suite Coreservers für den Versorgungsserver eingeben und Port 9971 angeben. Andernfalls sendet das Intel vPro-Gerät standardmäßig einen allgemeinen Broadcast, der nur empfangen werden kann, wenn Port 9971 vom Konfigurationsserver überwacht wird.

Der Standardbenutzername und das Standardkennwort für den Zugriff auf den Intel AMT-Konfigurationsbildschirm lauten "admin" und "admin". Der Benutzername kann gleich bleiben, aber das Kennwort muss bei der Versorgung in ein sicheres Kennwort geändert werden. Das neue Kennwort wird wie in den nachstehenden Schritten beschriebenen im Dialogfeld "Intel vPro - Allgemeine Konfiguration" eingegeben. Nachdem alle Geräte konfiguriert wurden, können Sie das Kennwort einzeln für jedes Gerät ändern. Für die Versorgung müssen Sie jedoch das Kennwort aus dem Dialogfeld "Allgemeine Konfiguration" verwenden.

Wenn die oben angegebenen Informationen in den Intel AMT-Konfigurationsbildschirm eingegeben wurden, sendet das Gerät Grußnachrichten, wenn es zum ersten Mal an das Netzwerk angeschlossen wird und versucht, mit dem Versorgungsserver zu kommunizieren. Wenn der Versorgungsserver diese Nachricht empfängt, beginnt der Versorgungsprozess, sobald der Server eine Verbindung zum verwalteten Gerät herstellt.

Nachdem der Coreserver die Grußnachricht empfangen und die PID geprüft hat, stellt er das Intel vPro-Gerät für den TLS-Modus bereit. Der TLS-Modus (Transport Layer Security) stellt einen sicheren Kommunikationskanal zwischen dem Coreserver und dem verwalteten Server zur Verfügung, während die Versorgung abgeschlossen wird. Bei diesem Prozess wird u. a. ein Datensatz mit der UUID und den verschlüsselten Anmeldeinformationen des Geräts in der Datenbank erstellt. Wenn die Daten für das Gerät in der Datenbank abgelegt wurden, erscheint das Gerät in der Liste nicht verwalteter Geräte.

Wenn ein Intel vPro-Gerät vom Coreserver versorgt wurde, kann es allein mit den Intel vPro-Funktionen verwaltet werden. Hierfür können Sie das Gerät aus der Liste nicht verwalteter Geräte auswählen und zu Ihren verwalteten Geräten hinzufügen. Alternativ können Sie auch Verwaltungsagenten auf dem Gerät bereitstellen, um zusätzliche Verwaltungsfunktionen einzusetzen.

Das empfohlene Versorgungsverfahren für Intel vPro-Geräte wird im Folgenden beschrieben.

1. Geben Sie ein neues sicheres Kennwort für die Versorgung von Intel vPro-Geräten ein.
2. Generieren Sie einen Satz Intel vPro-Versorgungskennungen (PID und PPS). Drucken Sie die Schlüsselliste aus oder exportieren Sie die Schlüssel auf ein USB-Laufwerk.
3. Melden Sie sich vom BIOS aus im Intel ME-Konfigurationsbildschirm des Geräts an und ändern Sie das Standardkennwort in ein sicheres Kennwort.
4. Melden Sie sich im Intel AMT-Konfigurationsbildschirm an. Geben Sie ein PID-/PPS-Schlüsselpaar aus der ausgedruckten Liste von Versorgungskennungen ein. Geben Sie die IP-Adresse des Coreservers (Versorgungsservers) ein und geben Sie Port 9971 an. Vergewissern Sie sich, dass für die Versorgung der Enterprise-Modus ausgewählt ist. Geben Sie den Hostnamen des Intel vPro-Geräts ein.
5. Beenden Sie den BIOS-Bildschirm. Das Gerät beginnt mit dem Senden von Grußnachrichten ("hello").
6. Der Coreserver empfängt eine Grußnachricht und gleicht die PID mit der Liste der generierten Schlüssel ab. Wenn eine Übereinstimmung registriert wird, versorgt er das Gerät.
7. Daraufhin wird das Gerät der Liste nicht verwalteter, erkannter Geräte hinzugefügt.
8. Wählen Sie das Gerät aus und fügen Sie es Ihren verwalteten Geräten hinzu (klicken Sie auf der Symbolleiste auf **Ziel**, klicken Sie auf die Registerkarte **Verwalten** und klicken Sie dann auf **Verschieben**). Sie können das Gerät als agentenfreies Gerät verwalten, oder Sie können zur Bereitstellung zusätzlicher Verwaltungsfunktionen Verwaltungsagenten auf dem Gerät bereitstellen.

Ausführliche Anweisungen zu Schritt 1 finden Sie unter "Ändern des Intel vPro-Kennworts" auf Seite 880.

Ausführliche Anweisungen zu Schritt 2 finden Sie unter "Generieren eines Satzes von Intel vPro-Versorgungskennungen" auf Seite 883.

Fehler im Versorgungsprozess

Wenn Sie einen nicht ordnungsgemäß gepaarten PID- und PPS-Satz eingeben (d. h. der PPS-Schlüssel passt nicht zum PID-Schlüssel), erscheint eine Fehlermeldung im Alarmprotokoll, und die Versorgung des betroffenen Geräts wird nicht fortgesetzt. Sie müssen das Gerät neu starten und ein korrektes PID-/PPS-Paar im Intel AMT-Konfigurationsbildschirm eingeben.

Wenn der Intel AMT-Konfigurationsbildschirm bei der Eingabe eines PID- oder PPS-Schlüssels eine Fehlermeldung anzeigt, haben Sie sich beim PID oder PPS vertippt. Die PID- und PPS-Schlüssel werden mit einer Prüfsumme überprüft.

Generieren eines Satzes von Intel vPro-Versorgungskennungen

WICHTIG: Bevor Sie Intel vPro-Kennungen generieren, müssen Sie zunächst ein Intel vPro-Kennwort für das standardmäßige "admin"-Konto erstellen und das Kennwort mit allen verwalteten Intel vPro-Geräten synchronisieren. See "Ändern des Kennworts für Intel vPro-Geräte" on page 879.

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > Kennungserzeugung**.
2. Geben Sie die Anzahl der zu generierenden Kennungen ein (in der Regel ist das die Anzahl von Geräten, die bereitgestellt werden sollen).
3. Wenn Sie ein anderes Präfix für die PIDs bevorzugen, geben Sie dieses in das Textfeld **PID-Präfix** ein. Dieses Präfix darf nur Großbuchstaben und Zahlen aus dem ASCII-Zeichensatz enthalten. Es können maximal 7 Zeichen für ein Präfix eingegeben werden.
4. Geben Sie einen Batchnamen für diese Gruppe generierter Kennungen ein.
5. Klicken Sie auf **Kennungen generieren**.
6. Wenn die Kennungen generiert wurden, klicken Sie auf **Kennungsliste drucken**, um die Liste der Kennungen zu drucken. (Es werden nur die derzeit in der Liste angezeigten Kennungen ausgedruckt.) Die Druckfunktion Ihres Browsers wird automatisch geöffnet.
7. Um alle bereits generierten Kennungen anzuzeigen, wählen Sie **Alle anzeigen** in der Liste **Batch-IDs anzeigen**.
8. Um einen Batch von generierten Kennungen anzuzeigen, wählen Sie den Batchnamen in der Liste **Batch-IDs anzeigen**.
9. Um eine Liste der generierten Kennungen zum späteren Nachschlagen zu drucken, klicken Sie auf **Kennungsliste drucken**. Das Windows-Dialogfeld zum Drucken wird geöffnet. Wählen Sie einen Drucker aus und klicken Sie auf **Drucken**.

Die Versorgungsschlüssel werden zum künftigen Gebrauch bei der Versorgung neuer Intel vPro-Geräte in der Datenbank gespeichert. Wenn Geräte bereitgestellt und die Versorgungsschlüssel aufgebraucht werden, werden die bereits verbrauchten Kennungen auf der Seite **Intel vPro-Kennungen generieren** schattiert dargestellt, damit Sie den Überblick behalten.

Hinweise zu Versorgungsschlüsseln

Damit Sie Kennungen leichter als PIDs identifizieren können, wird ein PID-Präfix hinzugefügt. Es muss jedoch nicht verwendet werden. Wir empfehlen 0 bis 4 Zeichen; die Maximalzahl für das Präfix ist 7 Zeichen.

Um Batches mit Versorgungsschlüsseln zu identifizieren, geben Sie einen Batchnamen ein. Dieser Name sollte beschreibend sein und angeben, auf welche Geräte sich die Kennungen beziehen. So können Sie zum Beispiel Batches für jede Organisation innerhalb Ihres Unternehmens generieren und diese als "Entwicklung", "Marketing", "Finanzen" usw. bezeichnen. Wenn Sie später die generierten Kennungen einsehen möchten, geben Sie den Batchnamen ein und klicken auf **Batch-IDs anzeigen**, um eine Liste mit nur diesen Kennungen anzuzeigen.

Klicken Sie hier, um eine Beschreibung der Intel vPro-Optionen anzuzeigen.

Kennungen generieren

Diesen Abschnitt verwenden Sie, um die Kriterien für die Generierung der PID und der PPS einzugeben.

- **Anzahl der zu generierenden Kennungen**: Geben Sie die Anzahl der zu generierenden Kennungen ein (in der Regel ist das die Anzahl von Geräten, die versorgt werden sollen). Sie müssen einen Wert eingeben, sonst können die Kennungen nicht generiert werden.
- **PID-Präfix für generierte Kennungen**: Geben Sie ein Präfix ein, anhand dessen Sie die PIDs leichter identifizieren können. Damit Sie Kennungen leichter als PIDs identifizieren können, wird ein PID-Präfix hinzugefügt. Es muss jedoch nicht verwendet werden. Wir empfehlen 0 bis 4 Zeichen; die Maximalzahl für das Präfix ist 7 Zeichen.
- **Batchname für generierte Kennungen**: Geben Sie einen Namen ein, anhand dessen das Batch mit generierten Kennungen identifiziert werden kann. Dieser Name ist optional. Der Name sollte beschreibend sein und angeben, auf welche Geräte sich die Kennungen beziehen. So können Sie zum Beispiel Batches für jede Organisation innerhalb Ihres Unternehmens generieren und diese als "Entwicklung", "Marketing", "Finanzen" usw. bezeichnen. Wenn Sie später die generierten Kennungen einsehen möchten, geben Sie den Batchnamen ein und klicken auf **Batch-IDs anzeigen**, um eine Liste mit nur diesen Kennungen anzuzeigen.

Batch-IDs anzeigen

Wenn Sie Namen für verschiedene Batches mit generierten Kennungen eingeben, werden die Namen in der Dropdownliste **Batch-IDs anzeigen** angezeigt. Die Kennungen, die unter dem ausgewählten Batchname zur Verfügung stehen, werden in dem Listenfeld unterhalb der Dropdownliste angezeigt. Wenn Sie keine Kennungen mit einem Batchnamen generieren, werden sämtliche Kennungen in dem Listenfeld angezeigt.

Diese Kennungen werden zum künftigen Gebrauch bei der Versorgung neuer Intel vPro-Geräte in der Datenbank gespeichert. Wenn Geräte versorgt und die Versorgungsschlüssel aufgebraucht werden, werden die bereits verbrauchten Kennungen auf der Seite **Intel vPro-Kennungen generieren** schattiert dargestellt, damit Sie den Überblick behalten.

Kennungen importieren/exportieren

Die von Ihnen generierten IDs können in eine Datei namens setup.bin exportiert werden. Die Datei setup.bin kann auf einem USB-Laufwerk gespeichert und zu anderen Versorgungsservern transportiert werden, so dass die Kennungen, die noch nicht verwendet wurden, importiert und für andere Intel vPro-Geräte eingesetzt werden können.

Kennungsliste drucken

Die Funktion "Kennungsliste drucken" druckt die Kennungen, die derzeit in der Liste angezeigt werden. Wenn Sie in der Dropdownliste **Batch-IDs anzeigen** die Option **Alle anzeigen** oder **Kein Batchname** ausgewählt haben, werden sämtliche verfügbaren Kennungen gedruckt. Wenn Sie einen Batchnamen aus der Dropdownliste **Batch-IDs anzeigen** auswählen, werden nur die Kennungen gedruckt, die in diesem Batch enthalten sind.

Importieren und Exportieren von Versorgungskennungen

Sie können Versorgungskennungen generieren und mithilfe eines USB-Laufwerks in eine Schlüsseldatei exportieren, um Intel vPro-Geräte zu versorgen. Die exportierten Kennungen werden in einer setup.bin-Datei gespeichert, die Sie in ein USB-Laufwerk kopieren können. Mit diesem USB-Laufwerk können Sie beim Versorgen neuer Intel vPro-Geräte automatisch die PID/PPS-Felder in Intel AMT BIOS auffüllen, bevor Sie die Geräte erkennen lassen und verwalten.

Wenn ein Gerätehersteller Ihnen einen Satz Versorgungskennungen für die von Ihnen erworbenen Intel vPro-Geräte zur Verfügung stellt, können Sie diese Kennungen in die Coredatenbank importieren. Auf diese Weise identifiziert der Coreserver diese Geräte als Intel vPro-Geräte und erkennt sie automatisch.

Diese beiden Prozesse werden nachstehend beschrieben.

Exportieren von Versorgungskennungen zur Verwendung mit einem USB-Laufwerk

Management Suite erstellt Versorgungskennungen (PID/PPS-Paare), die Sie zur Versorgung neuer Intel vPro-Geräte verwenden. Sie können eine Liste der generierten Kennungen drucken und sie bei der Versorgung der einzelnen Geräte manuell eingeben. Alternativ können Sie die Kennungen in eine "setup.bin"-Schlüsseldatei exportieren, diese Datei in einem USB-Laufwerk speichern und dann das USB-Laufwerk zur Versorgung der Geräte verwenden. Mit diesem Verfahren lassen sich Fehler bei der Versorgung vermeiden, da die Kennungen nicht manuell an jedem Gerät eingegeben werden müssen.

Das von Ihnen verwendete USB-Laufwerk muss mit FAT-16 formatiert sein, da dieses Verfahren andernfalls nicht funktioniert.

Die setup.bin-Datei wird mit einem von Intel definierten Schlüsseldateiformat erstellt. Beim Versorgen des neuen Intel vPro-Geräts verbinden Sie das USB-Laufwerk mit dem Gerät und starten es neu. Während des Bootvorgangs wird ein Kennungspaar (PID und PPS) aus der setup.bin-Datei entnommen und in das Intel AMT BIOS des Gerät eingegeben. Sobald das Gerät seine "Hello"-Nachricht im Netzwerk übermittelt, erkennt der Coreserver das Gerät und kann sicher mit ihm kommunizieren, da die Versorgungskennungen in der Coredatenbank vorhanden sind.

So exportieren Sie einen Stapel Versorgungskennungen zur Verwendung mit einem USB-Laufwerk

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > Kennungserzeugung > Kennungen importieren/exportieren**.
2. Wählen Sie **AMT-Kennungen in setup.bin-Datei exportieren**. Die Anzahl der Kennungen, die für den Export verfügbar sind, werden neben dieser Option in Klammern angezeigt.

3. Geben Sie das Kennwort für die vPro Management Engine ein und bestätigen Sie es. Mit diesem Kennwort können Sie auf die Intel vPro-Verwaltungsfunktionen zugreifen. Das Standardkennwort lautet "admin", falls Sie nicht bereits ein anderes Kennwort für die Management Engine festgelegt haben.
4. Geben Sie eine Zahl in das Textfeld **Anzahl der zu exportierenden Kennungen** ein. Sie müssen mindestens "1" in dieses Feld eingeben. Die höchste Zahl, die Sie hier eingeben können, entspricht der Anzahl der verfügbaren Kennungen, die neben der Option **AMT-Kennungen in Datei setup.bin exportieren** angezeigt wird.
5. Geben Sie in das Textfeld **Geben Sie den Speicherort für setup.bin an** einen Pfad ein oder navigieren Sie zu dem Ordner, in dem Sie die Datei setup.bin speichern wollen.

   Sie können die Datei in einem beliebigen Verzeichnis speichern und dann in ein USB-Laufwerk kopieren, oder Sie können ganz einfach das Verzeichnis des USB-Laufwerks angeben, sofern es mit dem Coreserver verbunden ist. Um die setup.bin-Datei zur Versorgung zu verwenden, muss sie im Stammverzeichnis des USB-Laufwerks gespeichert werden.
6. Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

HINWEIS: Die von Ihnen generierten Kennungen werden zusammen mit anderen Kennungen, die Sie generiert haben, auf der Seite **Intel vPro-Kennungen generieren** aufgelistet. Die Kennungen sind in der Liste abgeblendet, um zu signalisieren, dass sie für die Versorgung anderer Geräte nicht zur Verfügung stehen.

So verwenden Sie exportierte Versorgungskennungen auf neuen Intel vPro-Geräten

1. Exportieren Sie einen Batch Versorgungskennungen wie weiter oben beschrieben und speichern Sie die setup.bin-Datei im Stammverzeichnis eines USB-Laufwerks.
2. Verbinden Sie an jedem neuen Intel vPro-Gerät das USB-Laufwerk mit dem Gerät und starten Sie es neu.

Beim Booten greift das Gerät auf die setup.bin-Datei zu und entnimmt ein verfügbares Kennungspaar (PID und PPS) zur Verwendung im Versorgungsprozess. Anschließend kennzeichnet das Gerät das Kennungspaar als in Gebrauch, sodass es von keinem anderen Gerät verwendet wird. Das nächste Gerät, das Sie versorgen, verwendet dann das nächste verfügbare Kennungspaar.

Beachten Sie, dass der Standardbenutzername und das Kennwort für den Zugriff auf das Intel AMT BIOS unverändert geblieben sein müssen (Standard ist im Allgemeinen "admin/admin"), damit dieser Prozess ordnungsgemäß funktioniert. Sie sollten nicht bereits Versorgungskennungen auf dem Gerät eingegeben haben.

Importieren von Versorgungskennungen aus einer Schlüsseldatei in die Coredatenbank

Wenn ein Gerätehersteller Ihnen einen Satz Versorgungskennungen für die von Ihnen erworbenen Intel vPro-Geräte zur Verfügung stellt, können Sie diese Kennungen in die Coredatenbank importieren. Auf diese Weise identifiziert der Coreserver diese Geräte als Intel vPro-Geräte und erkennt sie automatisch. Der Hersteller stellt diese Kennungen (IDs) beim Kauf der Geräte in einer setup.bin-Schlüsseldatei bereit.

Um die Kennungen in die Coredatenbank zu importieren, navigieren Sie zu dem Verzeichnis der setup.bin-Datei, die der Hersteller bereitgestellt hat (kann eine CD oder DVD sein; oder Sie kopieren die Datei in ein beliebiges Laufwerk). Sobald diese Kennungen in der Datenbank gespeichert wurden und die Intel vPro-Geräte nach ihrem Start eine Grußnachricht gesendet haben, erkennt der Coreserver die Geräte.

So importieren Sie Versorgungskennungen aus einer Schlüsseldatei in die Coredatenbank

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > Kennungserzeugung > Kennungen importieren/exportieren**.
2. Wählen Sie **Aus USB-Schlüsseldatei importieren**.
3. Geben Sie in das Textfeld **Geben Sie den Speicherort für setup.bin an** einen Pfad ein oder navigieren Sie zu dem Ordner, der die Datei setup.bin enthält.
4. Klicken Sie auf **Übernehmen** und dann auf **Schließen**.

Die Versorgungskennungen werden der Coredatenbank hinzugefügt und im Dialogfeld **Intel vPro-Kennungen generieren** aufgelistet.

Verwenden der Remoteversorgung (Zero-Touch-Versorgung)

Dieser Abschnitt beschreibt die Remoteversorgung von Geräten mit Intel vPro 2.2/2.6 und höher.

Mit der Remoteversorgung können Sie ein Gerät im Werkszustand durch das Setupverfahren konfigurieren und dann das Intel AMT-Profil hinzufügen, damit das Gerät zur Out-of-Band-Verwaltung bereit ist. Wenn das Gerät zum ersten Mal hochgefahren wird und mit einem Netzwerk verbindet, beginnt es, Grußmeldungen zum Setup- und Konfigurationsserver zu senden (wenn Sie Geräte mit LANDesk Produkten verwalten, ist der Coreserver der Setup- und Konfigurationsserver). Wenn der Setup- und Konfigurationsserver läuft, stellt er eine sichere Verbindung zum Intel vPro-Gerät her und beginnt die Versorgung.

Wenn dieser Prozess erfolgreich ist, wird das Gerät der Liste erkannter Geräte hinzugefügt und kann vom Coreserver aus verwaltet werden. Wenn nur die Intel vPro-Funktionalität vorhanden ist, ist nur beschränkte Verwaltung möglich. Sie können auf dem Gerät jedoch für vollständige Verwaltungsfunktionen auch einen Managementagenten bereitstellen.

Die Remoteversorgung setzt zwei Bedingungen voraus:

- Das Netzwerk muss mit DHCP ausgestattet sein, wobei ein DNS-Eintrag den Coreserver als "Versorgungsserver" erkennen lässt.
- Auf dem Coreserver muss ein Intel Clientsetup-Zertifikat für die Domäne installiert sein, auf der der Coreserver installiert ist (nachstehend finden Sie Anweisungen für den Erwerb und die Installation eines Zertifikats).

Verzögerte Versorgung

Wenn ein Intel vPro-Gerät hochgefahren wird, aber nach einer gewissen Zeit keine Reaktion vom Setup- und Konfigurationsserver erhält (normalerweise 6 bis 12 Stunden, je nach Herstellereinstellung), beendet es das Senden der Grußpakete und wartet. Die Intel vPro-Funktionalität wird dann auf dem Gerät nicht aktiviert.

Um ein Gerät in diesem Zustand zu versorgen, können Sie darauf einen LANDesk Standard-Managementagenten installieren. Wenn der Agent feststellt, dass das Gerät Intel vPro-Funktionen besitzt, aktiviert er die Intel vPro-Funktionalität auf dem Gerät und sendet einen Ruf an den Webservice auf dem Coreserver, um ein Grußpaket zu empfangen. Der Versorgungsprozess wird dann vom Coreserver aus eingeleitet.

Bare-Metal-Versorgung

Intel vPro 3.0-Geräte und neuere Revisionen unterstützen einen "Bare-Metal" (oder agentenlosen) Ansatz der Remotekonfiguration. Wenn der Setup- und Konfigurationsserver richtig eingerichtet ist, ein DNS-Eintrag und das richtige Zertifikat auf dem Coreserver installiert ist, kann die Konfiguration ohne Agenten durchgeführt werden.

HINWEIS: Wenn das Intel vPro-Gerät hochgefahren wird, aber keine der oben beschriebenen "hello"-Grußmeldungen sendet, ist auf dem Gerät möglicherweise keine Remotekonfiguration aktiviert. Es hängt davon ab, ob der Hersteller die Remotekonfiguration aktiviert hat, indem er den Verwaltungsmodus des Geräts auf "AMT" gestellt hat. Sollte dies der Fall sein, können Sie auf dem Gerät einen LANDesk Managementagenten bereitstellen, um die Intel vPro-Funktionalität zu aktivieren und das Gerät versorgen (wie oben unter "Verzögerte Versorgung" beschrieben).

Hostgestützte Versorgung für Intel vPro 6.2 und höher

Management Suite verwendet hostgestützte Versorgung von Intel vPro-Geräten mit AMT-Version 6.2 oder höher. Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben, aber keine PID auf den Geräten festgelegt wurde bzw. kein Zero-Touch-Zertifikat bereitgestellt wurde, werden Ihre Geräte unter Verwendung des Clientsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in gewisser Hinsicht ein und spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen des Gerätesetups erforderlich ist.

Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben und entweder eine PID auf den Geräten festgelegt oder ein Zero-Touch-Zertifikat bereitgestellt haben, werden die Geräte unter Verwendung des Adminsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in keinerlei Weise ein und spiegelt den höheren Grad an Vertrauenswürdigkeit wider, der mit dem Gerätesetup einhergeht.

Beschaffung und Installation eines Intel Clientsetup-Zertifikats

Jeder Setup- und Konfigurationsserver benötigt ein Intel Clientsetup-Zertifikat. Das Zertifikat muss von einem autorisierten Zertifikatanbieter gekauft werden und einer unterstützten Klasse entsprechen. Die folgenden Anbieter sind für LANDesk Produkte für die folgenden Geräte zugelassen.

HINWEIS: Bevor Sie ein Zertifikat kaufen, sehen Sie in den Unterlagen oder den Supportinformationen des Anbieters nach, welche Zertifikate auf ihrem Gerät unterstützt werden.

Anbieter/Zertifikatklasse	Intel-Geräte	Acer-Geräte	Lenovo-Geräte
Go Daddy Klasse 2 CA	X	X	X
VeriSign Klasse 3 Primary CA-G3	X	X	X
VeriSign Klasse 3 Primary CA-G1	X	X	X
Comodo AAA CA	X	X	
Starfield Klasse 2 CA			X

Wenn Sie ein Zertifikat erwerben, müssen Sie eine CSR-Datei vorlegen (Certificate Signing Request). Diese Datei wird zusammen mit einer privaten Schlüsseldatei für Ihr LANDesk Produkt generiert. Nachdem Sie die Zertifikatdateien vom Anbieter erhalten, wird die private Schlüsseldatei in einem Verzeichnis mit einer freigegebenen, öffentlichen Schlüsseldatei und der Zertifikatdatei des Anbieters gespeichert. Dieses Verfahren wird nachstehend beschrieben.

So beschaffen und installieren Sie ein Intel Clientsetup-Zertifikat

1. Wählen Sie einen Anbieter aus und melden Sie sich auf seiner Webseite an.
2. Generieren Sie eine CSR-Datei und einen privaten Schlüssel: Führen Sie im Verzeichnis \Programme\LANDesk\ManagementSuite\amtprov die Datei AMTProvMgr2.exe mit folgenden Argumenten aus:
   `AMTProvMgr2.exe -domainName name.domain.com -country [zweistelliger Ländercode] -state [Name des Bundesstaats/-lands] -city [Name der Stadt] -organization [Name der Organisation]`
   Die Argumenten, die Sie angeben müssen, können von Anbieter zu Anbieter variieren. Der von Ihnen angegebene Domänenname sollte einen Namensraum enthalten. Um die Hilfeinformationen zu den Argumenten und dieser ausführbaren Datei aufzurufen, führen Sie die EXE-Datei von einer Eingabeaufforderung aus mit dem Argument -h aus.

   Diese ausführbare Datei speichert zwei Dateien im Verzeichnis "amtprov": certreq.csr (Certificate Signing Request) und corecakey.pem (eine private Schlüsseldatei).
3. Öffnen Sie die Datei certreq.csr in einem Texteditor und kopieren Sie ihren Inhalt.
4. Fügen Sie auf der Website des Anbieters den Inhalt der certreq.csr-Datei in das dafür vorgesehene Feld ein und vervollständigen Sie den Antrag für das Zertifikat.

   Nachdem Ihre Zertifikatanforderung verarbeitet wurde, erhalten Sie vom Anbieter zwei Dateien: eine Stammzertifikatdatei (eine allgemeine oder öffentliche Datei) und eine Zertifikatdatei für die von Ihnen angegebene Domäne.
5. Kopieren Sie die Stammzertifikatdatei des Anbieters und nennen Sie die Kopie `trusted_cert.pem`.
6. Kopieren Sie die Zertifikatdatei des Anbieters für Ihre Domäne und nennen Sie die Kopie `corecacert.pem`.
7. Speichern Sie die beiden o.g. Dateien zusammen mit der Datei `corecakey.pem` (oben in Schritt 2 generiert) in einem Ordner unter LDMAIN\amtprov\certStore\cert_1. Sie können bis zu acht Zertifikate in Unterordnern namens cert_1, cert_2 u.s.w. speichern.
8. Wenn Sie über weitere Konsolen verfügen, kopieren Sie diese drei Dateien in den selben Verzeichnispfad auf allen weiteren Konsolen.

Hostgestützte Versorgung

Management Suite verwendet hostgestützte Versorgung von Intel vPro-Geräten mit AMT-Version 6.2 oder höher. Dieses Thema beschreibt, wie dieser Prozess funktioniert und wie Sie ein Gerät aus dem Clientsteuerungsmodus in den Adminsteuerungsmodus überführen.

Der Versorgungsprozess

Für jedes Intel vPro-Gerät mit AMT Version 6.2 und höher führt Management Suite eine hostgestützte Versorgung des Geräts durch, sobald das Gerät erkannt und ein Intel vPro-Kennwort in das Dialogfeld "Intel vPro - Allgemeine Konfiguration" eingegeben wurde.

Sie müssen ein Kennwort eingeben, damit dieser Versorgungsprozess startet, und die Intel vPro-Treiber müssen unter Windows auf dem Gerät installiert worden sein. Darüber hinaus sind jedoch keine weiteren Tasks erforderlich, damit diese grundlegende Versorgung stattfinden kann.

Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben, aber keine PID auf den Geräten festgelegt wurde bzw. kein Zero-Touch-Zertifikat bereitgestellt wurde, werden Ihre Geräte unter Verwendung des Clientsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in gewisser Hinsicht ein und spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen des Gerätesetups erforderlich ist.

Wenn Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" ein Kennwort eingegeben haben und entweder eine PID auf den Geräten festgelegt oder ein Zero-Touch-Zertifikat bereitgestellt haben, werden die Geräte unter Verwendung des Adminsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in keinerlei Weise ein und spiegelt den höheren Grad an Vertrauenswürdigkeit wider, der mit dem Gerätesetup einhergeht.

HINWEIS: Management Suite überprüft nicht, ob ein Zero-Touch-Zertifikat gültig ist oder innerhalb der aktuellen Domäne funktioniert. Es wird lediglich das Vorhandensein eines Zertifikats kontrolliert. Wenn Ihr Zertifikat aus irgendeinem Grunde ungültig ist, wird die Versorgung im Clientsteuerungsmodus fortgesetzt.

Wenn Sie im Zweifel sind, welcher Steuerungsmodus bei einem Intel vPro-Gerät wirksam ist, können Sie sich den Intel vPro-Status des Geräts anzeigen lassen. (Hierzu klicken Sie mit der rechten Maustaste in der Netzwerkansicht und wählen **Intel vPro-Optionen > Intel vPro-Status**.)

Wechsel vom Clientsteuerungsmodus in den Adminsteuerungsmodus

Wenn Geräte vorhanden sind, die im Clientsteuerungsmodus versorgt wurden, und Sie installieren zu einem späteren Zeitpunkt ein Zero-Touch-Zertifikat, dann können Sie die Geräte im Adminsteuerungsmodus erneut versorgen.

So versorgen Sie ein Intel vPro 6.2+-Gerät erneut

1. Installieren Sie ein Zero-Touch-Zertifikat auf dem Coreserver.
2. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf ein Intel vPro-Gerät und wählen Sie **(Erneutes) Setup und Konfiguration von vPro** aus.

Management Suite versorgt das Gerät dann in den Adminsteuerungsmodus.

Unterschiede zwischen Clientsteuerungsmodus und Adminsteuerungsmodus

Der Clientsteuerungsmodus beschränkt die Intel vPro-Funktionalität, die auf einem verwalteten Gerät zur Verfügung steht. Dies spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen der Geräteversorgung erforderlich ist. Die folgende Liste beschreibt die Beschränkungen des Clientsteuerungsmodus.

- Die Funktion "System Defense" ist nicht verfügbar.
- Umleitungsaktionen (IDE-R und KVM) mit Ausnahme der Initiierung einer SOL-Sitzung und Änderungen der Bootoptionen (einschließlich Boot nach SOL) erfordern vorab die Zustimmung des Benutzers. Das IT-Supportpersonal kann dennoch unter Verwendung von Intel AMT Probleme von Endbenutzern remote lösen.

- Wenn ein Benutzer vom Typ "Auditor" definiert wurde, ist keine Auditorberechtigung erforderlich, um die Versorgung rückgängig zu machen.
- Bei anderen Funktionen wird die Ausführung blockiert, damit ein nicht vertrauenswürdiger Benutzer keinesfalls die Kontrolle über die Plattform erlangen kann.

Wenn Sie ausführlichere Informationen wünschen, sollten Sie die neuste Version des *Intel AMT Implementation and Reference Guide* zu Rate ziehen. Dieses Implementierungs- und Referenzhandbuch für Intel AMT finden Sie auf der Intel Website.

Verwenden der Intel vPro-Energieoptionen

Management Suite umfasst Optionen zum Ein- und Ausschalten von Intel vPro-Geräten. Sie können diese Optionen auch dann verwenden, wenn das Betriebssystem eines Geräts nicht reagiert, solange das Gerät mit dem Netzwerk verbunden ist und über Standbystrom verfügt.

Wenn Management Suite Energieoptionsbefehle initiiert, lässt sich in manchen Fällen nicht verifizieren, ob die Befehle auf der Hardware, die den Befehl empfängt, unterstützt werden. Einige Geräte, die über Intel vPro verfügen, unterstützen ggf. nicht alle Energieoptionen (ein Gerät unterstützt möglicherweise IDE-R-Neustarts von einer CD, jedoch nicht von einer Floppy). Informieren Sie sich in der Dokumentation des Hardwareherstellers, wenn Sie den Eindruck haben, dass eine Energieoption auf einem bestimmten Gerät nicht funktioniert. Erkundigen Sie sich bei Intel auch über Firmware- oder BIOS-Aktualisierungen für das Gerät, wenn Energieoptionen nicht wie erwartet funktionsfähig sind.

Wenn bei Intel vPro-Geräten ein Einschaltbefehl erteilt wird, sendet Management Suite zunächst einen Intel vPro-Reaktivierungsbefehl. Ist dieser Befehl nicht erfolgreich, wird ein normaler Wake-on-LAN-Befehl an das Gerät gesendet.

Sie können einfach die Stromzufuhr des Geräts ein- oder ausschalten, oder Sie können einen Neustart ausführen und bestimmen, wie das Gerät neu gestartet wird. Die Optionen werden in der folgenden Tabelle beschrieben.

Option	Beschreibung
Power off (Ausschalten)	Schaltet die Stromzufuhr zum Gerät aus.
Power on (Einschalten)	Schaltet die Stromzufuhr zum Gerät ein.
Neustart	Schaltet den Strom auf dem Gerät aus und dann wieder ein.
Normaler Start	Startet das Gerät mit der Startsequenz, die als Standard auf dem Gerät eingestellt ist.
Von der lokalen Festplatte starten	Erzwingt einen Start von der Festplatte des Geräts aus, unabhängig vom Standardstartmodus auf dem Gerät.

Option	Beschreibung
Vom lokalen CD/DVD-Laufwerk starten	Erzwingt einen Start von der CD oder dem DVD-Laufwerk des Geräts aus, unabhängig vom Standardstartmodus auf dem Gerät.
PXE-Start	Wenn das PXE-aktivierte Gerät neu gestartet wird, sucht es einen PXE-Server im Netzwerk; wenn einer gefunden wird, wird eine PXE-Startsitzung auf dem Gerät gestartet.
IDE-R-Start	Startet das Gerät neu mit der ausgewählten IDE-Umleitungsoption (siehe nachstehender Hinweis).
BIOS-Setup beim Hochfahren öffnen	Wenn das Gerät gestartet wird, kann der Benutzer das BIOS-Setup eingeben.
Umleitungsfenster der Konsole anzeigen	Wenn das Gerät gestartet wird, wird es im seriellen Modus über dem LAN-Modus gestartet, um ein Konsolenumleitungsfenster anzuzeigen.
IDE-Umleitung: Von Diskettenlaufwerk neu starten	Das Gerät wird von dem angegebenen Diskettenlaufwerk gestartet.
IDE-Umleitung: Von CD/DVD neu starten	Das Gerät wird von dem angegebenen CD-Laufwerk gestartet.
IDE-Umleitung: Von einer angegebenen Abbilddatei neu starten	Das Gerät wird von der angegebenen Abbilddatei gestartet (Abbilddateien auf Diskette müssen im .img-Format und Abbilddateien auf CD im .iso-Format vorliegen; siehe Hinweis weiter unten).

So verwenden Sie die Intel vPro-Energieoptionen

1. Klicken Sie mit der rechten Maustaste in der Netzwerkansicht auf ein Intel vPro-Gerät und wählen Sie **Intel vPro-Optionen > Intel vPro-Remote-Bootmanager** aus.
2. Wählen Sie einen Energiebefehl aus.
3. Wenn Sie **Neustart** auswählen, wählen Sie eine Startoption.
4. Wenn Sie die IDE-Umleitung als Startmethode auswählen, geben Sie ein Disketten- bzw. CD-Laufwerk oder eine Abbilddatei an.
5. Wenn noch eine IDE-R-Sitzung geöffnet ist und Sie diese schließen möchten, klicken Sie auf **IDE-R-Sitzung schließen**.
6. Klicken Sie auf **Senden**, um den Strombefehl zu starten oder auf **Schließen**.

Hinweise zur Verwendung von IDE-Umleitungsoptionen

Bei Verwendung der IDE-Umleitungsoptionen müssen Disketten-Abbilddateien das Format .img und CD-Abbilddateien das Format .iso aufweisen. Einige BIOS erfordern unter Umständen, dass sich das CD-Abbild auf einer Festplatte befindet.

Intel vPro zeichnet im Normalfall die letzten IDE-R-Einstellungen auf; jedoch löscht Management Suite die Einstellungen nach 45 Sekunden, sodass die IDE-R-Funktion bei nachfolgenden Startvorgängen nicht gestartet wird. Die IDE-R-Sitzung auf einem Intel vPro-Gerät dauert 6 Stunden oder bis die Management Suite Konsole ausgeschaltet wird. Alle IDE-R-Vorgänge, die nach 6 Stunden noch nicht abgeschlossen sind, werden abgebrochen.

HINWEIS: In manchen Situationen kann der Eindruck entstehen, dass der IDE-R-Startvorgang auf der Serial-over-LAN (SOL)-Konsole in einen Timeout läuft, obwohl der Startvorgang eigentlich immer noch aktiv ist. Wenn bei einem Startabbild zu viel Zeit für die Initialisierung benötigt wird und das Senden von Daten an die SOL-Konsole zu lange dauert, stoppt die SOL-Konsole die Kommunikation und die Tastaturverbindung geht verloren. Dies passiert, wenn das fürs Starten verwendete Medium eine lange Antwortzeit hat und mehr als 60 Sekunden für die Initialisierung benötigt (dies ist der zulässige Timeout-Höchstwert). Wenn dieses Problem beim Starten mit einer Diskette oder mit einem anderen Medium auftritt, empfehlen wir, von einer Startabbilddatei (.img-Datei) zu starten, statt von einem herausnehmbaren Medium.

Remotezugriff für Intel vPro-Geräte

Intel vPro-Geräte (Version 4.0 und höher) können remote von einer LANDesk Management Suite-Konsole aus verwaltet werden. Wenn sich ein Intel vPro-Gerät außerhalb des Netzwerks befindet, in dem sich die Management Suite-Konsole befindet, wird die Kommunikation mit dem Coreserver – durch die Firewall und DMZ – durch die Remotezugriffsfunktionen ermöglicht.

Der Remotezugang für Intel vPro-Geräte ermöglicht die Kommunikation zwischen einer Verwaltungskonsole innerhalb eines sicheren Netzwerks und Intel vPro-Geräten außerhalb des Netzwerks. Die Kommunikation erfolgt durch einen TLS-Tunnel, der das Gerät außerhalb des Netzwerks mit einem Server (dem Intel vPro Gateway-Server) verbindet, der sich typischerweise in der DMZ des Netzwerks befindet. An den Intel vPro Gateway-Server gerichtete Kommunikation wird ihrerseits über sichere HTTP-Verbindungen unter Verwendung eines vertrauenswürdigen Stammzertifikats und eines Serverzertifikats an den Management Suite Coreserver gesendet.

Damit ein verwaltetes Gerät Remotezugriff verwenden kann, muss es über Folgendes verfügen:

- eine in der Firmware angewendete Richtlinie für den Remotezugriff
- ein vertrauenswürdiges Stammzertifikat, das dem für LANDesk Produkte verwendeten Coreserver-Zertifikat entspricht
- ein Clientzertifikat, das dem für LANDesk Produkte verwendeten Coreserver-Zertifikat entspricht

Mit Remotezugriffsfunktionen können Sie eine Richtlinie für den Remotezugriff erstellen und diese auf die Firmware der verwalteten Geräte anwenden.

Wenn Sie das Gerät konfiguriert und den Intel vPro Gateway-Server eingerichtet haben, werden Remotesitzungen vom verwalteten Gerät nach einem regelmäßigen, von Ihnen definierten Zeitplan geöffnet (typischerweise einmal pro Tag). Beim Initiieren einer Remotesitzung wird das Gerät im Dialogfeld "Konfiguration des Intel vPro-Remotezugriffs" in der Liste der geöffneten Sitzungen aufgeführt. Darüber hinaus zeigt die Clientstatusseite in Management Suite an, dass die Sitzung geöffnet ist.

HINWEIS: Beachten, Sie dass der Remotezugriff bei seiner ursprünglichen Entwicklung als "Client-Initiated Remote Access" bzw. "CIRA" bezeichnet wurde. Sollten Ihnen also Verweise auf CIRA begegnen, so beziehen sich diese auf den Remotezugriff. Der Intel vPro Gateway-Server wurde früher als "Management Presence Server (MPS)" bezeichnet, daher könnten Sie auch Verweise auf MPS sehen, wenn der Gateway-Server gemeint ist. Darüber hinaus könnte in der Intel-Dokumentation von "Fast Call for Help" die Rede sein, wobei sich dies auf die Remotezugriffsoption bezieht, die vom Clientgerät initiiert wird.

Einrichten eines Intel vPro Gateway-Servers

Sie können den Remotezugriff aktivieren, indem Sie einen Server in Ihrem Netzwerk als Intel Gateway-Server verwenden. Hierzu sind die folgenden beiden allgemeinen Tasks durchzuführen:

- Führen Sie eine ausführbare Installationsdatei auf einem Server aus und konfigurieren Sie ihn für den Einsatz als Intel vPro-Gateway-Server.
- Konfigurieren Sie die Optionen zur Konfiguration des Remotezugriffs und zur Erkennung der Netzwerkumgebung auf dem Management Suite Coreserver.

Die Dokumentation zur Einrichtung des Remotezugriffs befindet sich auf Ihrem Coreserver im Ordner \Programme\LANDesk\Management Suite\Install\vpro\remoteaccess. (Dies ist der Ordner, der die ausführbare Datei enthält.)

Konfigurieren des Remote-KVM-Zugriffs für Intel vPro-Geräte

Intel vPro-Geräte (AMT-Version 6 und höher) können remote über KVM-Zugriff verwaltet werden. Der IT-Administrator kann so den gesamten Bildschirm des Clientgeräts sehen und die Tastatur, die Maus und den Bildschirm des Geräts vollständig remote steuern.

Die KVM-Funktion bietet Unterstützung für zwei Verbindungsmodi: direkt und über einen Gateway (auch MPS genannt). Ferner unterstützt sie zwei Kommunikationstypen: TLS (Standard) und Non-TLS. Bei der Versorgung eines AMT-Geräts wird die KVM-Funktion standardmäßig deaktiviert. Die KVM-Funktion ist auf einen lizenzierten Core bzw. eine lizenzierte Konsole beschränkt. Auf einem eigenständigen Remote Control Viewer kann die KVM-Funktion nicht verwendet werden.

So konfigurieren Sie KVM-Einstellungen

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > KVM-Konfiguration**.
2. Zur Aktivierung von KVM klicken Sie im Feld **KVM-Aktivierung** auf **KVM aktivieren**.
3. Im Feld **Standardrichtlinie für die Zustimmung des Benutzers** wählen Sie **Zustimmung des Benutzers mit anschließendem Timeout aktiveren** und geben Sie die Anzahl der Sekunden an, nach denen ein Benutzer ein Einmalkennwort für den Konsolenbediener eingeben muss.
4. Wenn Sie sich entscheiden, die Option für die Zustimmung des Benutzers nicht zu verwenden, klicken Sie auf **Zustimmung des Benutzers deaktivieren**.
5. Geben Sie dann im Feld **Sitzungstimeout** einen Zahlenwert für die Anzahl der Minuten ein, für die eine TCP-Remotesteuerungssitzung inaktiv sein darf, bevor sie geschlossen wird. Dieses Feld ist deaktiviert, wenn die Option für die Zustimmung des Benutzers (im vorherigen Schritt) deaktiviert wurde.
6. Klicken Sie auf **OK**.

KVM-Beschränkungen

- KVM bietet keine Unterstützung für den Remotesteuerungs-Sicherheitstyp.
- Der Remotesteuerungs-Sicherheitstyp ist auf dem Clientgerät gespeichert. Der Authentifizierungsserver fordert den Client auf, den Sicherheitstyp zurückzugeben und entscheidet dann, ob der Remotesteuerungsbenutzer das Clientgerät steuern darf. Beim Herstellen der Verbindung zu ME gibt es keine Sicherheit bei der Rückkehr zum Authentifizierungsserver (Coreserver).
- KVM bietet keine Unterstützung für entsprechende Remotesteuerungsrichtlinien-Einstellungen.
- Für eine KVM-Verbindung können keine Remotesteuerungsrichtlinien vom Typ "Nur anzeigen" oder "Berechtigung erforderlich" angewendet werden. "Berechtigung erforderlich" kann wie "Zustimmungscode des Benutzers" in der AMT-Konfiguration behandelt werden und sollte über die AMT-Einstellung und nicht über "RCViewer" festgelegt werden.
- KVM bietet keine Unterstützung für die Remotesteuerungsoptionen in der Agentenkonfiguration.
- KVM bietet keine Unterstützung für Dateiübertragung, Remoteausführung, Chat- und Zeichenfunktionen über eine KVM-Verbindung.
- KVM bietet keine Unterstützung für den Remotesteuerungsoption "Bildschirm leeren".

Intel vPro-Netzwerksicherheitsrichtlinien

Intel vPro bietet eine System Defense-Funktion, die die Netzwerksicherheitsrichtlinien auf verwalteten Geräten durchsetzt. LANDesk® Management Suite wendet eine System Defense-Richtlinie auf Intel vPro-Geräte an. Jedes Gerät filtert eingehende und ausgehende Netzwerkpakete gemäß den definierten Richtlinien.

Ergibt sich zwischen Netzwerkverkehr und den in einem Filter definierten Alarmbedingungen eine Übereinstimmung, wird ein Alarm generiert und der Netzwerkzugriff des Geräts wird gesperrt. Das Gerät wird dann vom Netzwerk getrennt, bis Sie den Netzwerkzugriff für das Gerät unter Verwendung der Funktion "System Defense-Reparatur" wiederherstellen.

Anwenden von Intel vPro System Defense-Richtlinien

Wenn eine System Defense-Richtlinie auf einem verwalteten Gerät aktiv ist, überwacht das Gerät alle ein- und ausgehenden Netzwerkdaten. Wenn Filterbedingungen erkannt werden, geschieht Folgendes:

1. Das verwaltete Gerät sendet einen ASF-Alarm an den Coreserver und das Alarmprotokoll wird um einen Eintrag erweitert.
2. Der Coreserver stellt fest, gegen welche Richtlinie verstoßen wurde, und sperrt den Netzwerkzugriff auf verwalteten Geräten.
3. Das Gerät wird in der System Defense-Reparaturwarteschlange gelistet.
4. Um den Netzwerkzugriff auf dem Gerät wiederherzustellen, führt der Administrator die erforderlichen Reparaturschritte aus und entfernt dann das Gerät aus der Reparaturwarteschlange. Damit wird die System Defense-Richtlinie auf dem Gerät wiederhergestellt.

Intel vPro System Defense-Richtlinien

Die Intel vPro System Defense-Technologie gestattet die Netzwerkfilterung auf der Ebene des Intel AMT-Chips. Systeme, die nicht mehr sicher sind und eine Bedrohung für das Netzwerk darstellen, können remote unter Quarantäne gestellt werden, wobei bestimmte Ports und IP-Adressen für die Reparatur geöffnet bleiben, ohne dass dies eine Bedrohung für das übrige Netzwerk darstellt.

LANDesk Management Suite enthält die folgenden vordefinierten System Defense-Richtlinien.

- **BlockFTPSrvr:** Diese Richtlinie verhindert die Übermittlung von Netzwerkdaten über einen FTP-Port. Pakete, die von FTP-Port 21 gesendet bzw. dort in Empfang genommen werden, werden verworfen und der Netzwerkzugriff wird unterbrochen.
- **LDCBKillNics:** Diese Richtlinie blockiert Netzwerkdaten an allen Anschlüssen, mit Ausnahme der folgenden Verwaltungsanschlüsse:

Beschreibung des Anschlusses	Zahlenbereich	Datenrichtung	Protokoll
LANDesk Management	9593-9595	Senden/Empfangen	TCP, UDP
Intel vPro Management	16992-16993	Senden/Empfangen	Nur TCP
DNS	53	Senden/Empfangen	Nur UDP
DHCP	67-68	Senden/Empfangen	Nur UDP

  Wenn der Coreserver den Netzwerkzugriff auf einem verwalteten Gerät deaktiviert, bedeutet dies, dass diese Richtlinie auf das Gerät angewendet wird. Wird dann das Gerät aus der Reparaturschlange entfernt, so wird die ursprüngliche Richtlinie erneut auf das Gerät angewendet.
- **LDCBSYNFlood:** Diese Richtlinie erkennt einen SYN-Flooding Denial-of-Service-Angriff: Sie unterstützt maximal 10.000 TCP-Pakete mit eingeschaltetem SYN-Flag pro Minute. Bei Überschreitung dieses Wertes wird der Netzwerkzugriff deaktiviert.
- **UDPFloodPolicy:** Diese Richtlinie erkennt einen SYN-Flooding Denial-of-Service-Angriff: Sie unterstützt maximal 20.000 UDP-Pakete pro Minute auf Ports mit einer Nummer zwischen 0 und 1023. Bei Überschreitung dieses Wertes wird der Netzwerkzugriff deaktiviert.

Wiederherstellen des Netzwerkzugriffs für Intel vPro-Geräte

Wenn der Netzwerkzugriff eines Geräts aufgrund einer Situation deaktiviert wurde, die in Konflikt zu einer System Defense-Richtlinie steht, wird das betreffende Gerät in der Reparaturwarteschlange aufgelistet. Das Gerät bleibt so lange in der Liste, bis Sie es aus der Liste entfernen und dadurch die Richtlinie auf diesem Gerät reaktivieren.

Bevor Sie diesen Schritt ausführen, müssen Sie das Problem beheben, das dafür verantwortlich war, dass das Gerät zur Reparaturwarteschlange hinzugefügt wurde. Wurden beispielsweise FTP-Daten erkannt, müssen Sie sicherstellen, dass die entsprechenden Maßnahmen ergriffen werden, um weiteren FTP-Datenverkehr auf dem Gerät zu verhindern.

So stellen Sie den Netzwerkzugriff auf ein Gerät in der Reparaturwarteschlange wieder her

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > System Defense-Reparatur**.
2. Wählen Sie die Geräte aus, für die der Netzwerkzugriff wiederhergestellt werden kann, und klicken Sie auf **Reparieren**.

Mit dieser Aktion wird der Netzwerkzugriff wiederhergestellt und die System Defense-Richtlinien werden auf die ausgewählten Geräte angewendet.

Bearbeiten von Zeichenfolgen für die Intel vPro-Clientbenachrichtigung

Sie können einen Benutzer mit einer Nachricht davon in Kenntnis setzen, wenn Intel vPro System Defense ein Problem erkannt hat und das Gerät des Benutzers vom Netzwerk getrennt wurde. Beim Trennen eines Geräts vom Netzwerk wird ein Nachrichtenfeld angezeigt. Nachdem das Problem behoben und das Gerät wieder mit dem Netzwerk verbunden (d. h. vom Administrator aus der Reparaturwarteschlange entfernt) wurde, wird eine zweite Nachricht angezeigt.

Dieses Dialogfeld verwenden Sie zur Eingabe der Benachrichtigungstexte, die auf verwalteten Geräten angezeigt werden. Sie können den Standardbenachrichtigungstext verwenden oder die Nachricht Ihren Wünschen entsprechend anpassen.

So verwenden Sie Benachrichtigungen für Intel vPro System Defense

1. Klicken Sie auf **Konfigurieren > Intel vPro-Optionen > Zeichenfolgen für Clientbenachrichtigung**.
2. Markieren Sie das Kontrollkästchen **Aktiviert**, um Nachrichten zu senden, wenn der Netzwerkzugriff eines Geräts getrennt wird.
3. Falls Sie eine Nachricht anpassen möchten, ersetzen Sie einfach den Standardtext durch die Nachricht, die auf den Clientgeräten angezeigt werden soll.
4. Klicken Sie auf **OK**.

Intel vPro-Wireless-Unterstützung

Intel vPro-Geräte (Version 2.5 oder höher) mit Wireless-Funktionen können Out-of-Band über eine Wireless-LAN-Verbindung verwaltet werden, wenn sie eingeschaltet sind und die Wireless-Schnittstelle aktiv ist. Wenn sich ein Notebook im Energiesparmodus befindet, kann es nur dann Out-of-Band verwaltet werden, wenn es mit einem verkabelten LAN verbunden und an Netzstrom angeschlossen ist.

Wenn das Notebook eingeschaltet ist, kommuniziert der Intel AMT-Chip (Active Management Technology) im Notebook mit dem Wireless-LAN-Treiber. Wenn Intel AMT ein passendes Profil findet, leitet der Treiber den Datenverkehr, der an das Intel AMT-Gerät gerichtet ist, weiter. Auch wenn der Treiber ein Problem hat, kann Intel AMT Out-of-Band-Management-Verkehr von der Wireless-Netzwerk-Schnittstelle empfangen.

Intel vPro verwendet das Windows-Wirelessprofil des Geräts für das Wireless-Management.

Damit Intel AMT mit einer Wireless-LAN-Verbindung funktioniert, muss es dem Notebook seine IP-Adresse mitteilen. Dafür muss Intel AMT so konfiguriert sein, dass es DHCP verwenden kann und es muss ein DHCP-Server verfügbar sein, der die IP-Adressen verteilt. Wenn Intel AMT so konfiguriert ist, dass es statische IP-Adressen verwendet, wird die Wireless-Konnektivität deaktiviert.

Wenn ein Notebook erkannt und versorgt wird, während es mit einem verkabelten Netzwerk verbunden ist, kann es sofort über dieses Netzwerk verwaltet werden. Wenn das Notebook auf eine kabellose Verbindung umschaltet, kann es eine Verzögerung geben, bevor die Intel vPro-Verwaltung dafür aktiviert wird. Das liegt an einer Änderung in der Auflösung des Computernamens in der DNS des Netzwerks. Die Wireless-IP-Adresse des Notebooks ist eine andere als die IP-Adresse des verkabelten Netzes, daher kommt es zu einer Verzögerung, bevor die neue IP-Adresse für das Notebook mit dem Computernamen übereinstimmt.

Intel vPro - Allgemeine Konfiguration

Das Dialogfeld "Allgemeine Konfiguration" enthält Konfigurationsoptionen, die Sie definieren müssen, damit Sie Intel vPro-aktivierte Geräte verwalten können.

HINWEIS: Geben Sie ein Kennwort in dieses Dialogfeld ein, wenn Sie beabsichtigen, die Intel vPro-Funktionen für die betreffenden verwalteten Geräte zu aktivieren. Das Kennwort wird in der Datenbank gespeichert und global bei der Versorgung von Intel vPro-Geräten angewendet, d. h. Sie müssen mit der Einrichtung und Konfiguration der verschiedenen Versionen von Intel vPro-Geräten vertraut sein.

Setup und Konfiguration

Im Dialogfeld "Intel vPro - Allgemeine Konfiguration" können Sie das Kennwort ändern, das für das Standard-Administratorkonto verwendet wird. Dieses Kennwort wird für alle neuen Intel vPro-Geräte bei der Versorgung angewendet. Sie haben darüber hinaus die Option, dieses Kennwort auf allen derzeit verwalteten Intel vPro-Geräten zu ändern. Es empfiehlt sich, diese Option zu verwenden, damit alle Geräte dieselben Anmeldeinformationen aufweisen.

- **Kennwort**: Geben Sie ein sicheres Kennwort für die Kommunikation mit neuen Intel vPro-Geräten und deren Versorgung ein. Für Geräte, die Sie verwalten werden, sollte das "Admin"-Kennwort, das Sie auf dem Intel AMT-Konfigurationsbildschirm eingeben (der über das Geräte-BIOS angezeigt wird) mit dem Kennwort übereinstimmen, das Sie im Dialogfeld "Intel vPro - Allgemeine Konfiguration" eingegeben haben. Dieses Kennwort wird in der Datenbank gespeichert und global bei der Versorgung von Intel vPro-Geräten angewendet.
- **Dieses Kennwort synchronisieren**: Markieren Sie dieses Kontrollkästchen, wenn Sie die Änderung auf alle derzeit verwalteten vPro-Geräte anwenden möchten.
- **Non-TLS-Kommunikation verwenden**: Markieren Sie dieses Kontrollkästchen, wenn Sie sich für die Verwendung der weniger sicheren Non-TLS-Kommunikation in Verbindung mit Geräten entschieden haben, die im Enterprise-Modus konfiguriert sind. Diese Option wird aufgrund der Sicherheitsrisiken, die die Verwendung eines weniger sicheren Kommunikationsverfahrens mit sich bringen kann, nicht empfohlen.

Verwendung eines starken Kennworts

Die sichere Kommunikation bei Intel vPro erfordert ein starkes Kennwort. Kennwörter sollten folgende Anforderungen erfüllen:

- mindestens 8 Zeichen lang
- mindestens eine Zahl (0 bis 9)
- mindestens ein nicht alphanumerisches ASCII-Zeichen (z. B. !, &, %)
- lateinische Groß- und Kleinbuchstaben oder Nicht-ASCII-Zeichen (UTF+00800 und höher).

Automatische Versorgung für Intel vPro 6.2 und höher

Intel vPro-Geräte mit AMT-Version 6.2 oder höher werden von Management Suite automatisch versorgt. Wenn Sie in diesem Dialogfeld ein Kennwort eingegeben haben, aber keine PID auf den Geräten festgelegt wurde bzw. kein Zero-Touch-Zertifikat bereitgestellt wurde, werden Ihre Geräte unter Verwendung des Clientsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in gewisser Hinsicht ein und spiegelt den niedrigeren Grad an Vertrauenswürdigkeit wider, der für das Abschließen des Gerätesetups erforderlich ist.

Wenn Sie in diesem Dialogfeld ein Kennwort eingegeben haben und entweder eine PID auf den Geräten festgelegt oder ein Zero-Touch-Zertifikat bereitgestellt haben, werden die Geräte unter Verwendung des Adminsteuerungsmodus versorgt. Dieser Modus schränkt die Intel vPro-Funktionalität in keinerlei Weise ein und spiegelt den höheren Grad an Vertrauenswürdigkeit wider, der mit dem Gerätesetup einhergeht.

Timeout

In Ihrer Netzwerkumgebung ist unter Umständen ein höherer Timeoutwert für Kommunikationsaufrufe erforderlich, damit weniger Netzwerkfehler auftreten. Beachten Sie, dass eine Erhöhung des Timeoutwerts für Intel vPro-Aufrufe zur Folge haben kann, dass der Abschluss mancher Vorgänge unter Umständen mehr Zeit in Anspruch nehmen kann, wenn die Geräte nicht reagieren oder nicht mit dem Netzwerk verbunden sind.

- **Timeout**: Legt den Wert für die Zeit, die Intel vPro für Kommunikationsaufrufe im Netzwerk verwenden soll, in Sekunden fest. Der Mindestwert ist 5 Sekunden.

Konfigurieren der Erkennung der Netzwerkumgebung

Bei Intel vPro Remote Access wird die Domäne, mit der ein Gerät verbunden ist, entweder als innerhalb des Unternehmensnetzwerks oder als außerhalb der Unternehmensnetzwerks gelegen betrachtet. Dieses Dialogfeld listet gültige Domänen auf, die das Unternehmensnetzwerk definieren.

Wenn ein Intel vPro-Gerät (Revision 3.0 oder neuer) mit einer Domäne in dieser Liste verbunden ist, kann es direkt vom Coreserver verwaltet werden und kommuniziert mit dem Core über ganz normale Intel vPro-Verbindungen. Wenn das Gerät mit einer anderen Domäne verbunden ist, kann es nur über Intel vPro Remote Access verwaltet werden.

Standardmäßig werden Einstellungen für die Erkennung der Netzwerkumgebung nur auf diejenigen Intel vPro-Geräte angewendet, die mit Remote Access (Remotezugriff) ausgestattet sind. Wenn das Kontrollkästchen **NED-Einstellung nur auf Systeme anwenden, die für Remotezugriff konfiguriert sind** aktiviert ist, werden die Einstellungen nur auf Geräte mit Remote Access angewendet und für andere Intel vPro-Geräte ignoriert.

HINWEIS: Sie müssen an dieser Stelle alle gültigen Domänen in Ihrem Unternehmensnetzwert aufgelistet haben. Wenn Sie nicht alle gültigen Domänen auflisten, unterbrechen Sie damit unter Umständen die gesamte Intel vPro-Verwaltungskommunikation in Ihrem Netzwerk.

So fügen Sie eine Domäne zur Liste der genehmigten Domänen hinzu

1. Geben Sie den Domänennamen in das Textfeld **Genehmigte Domäne hinzufügen** ein.
2. Klicken Sie auf **Hinzufügen**.

So entfernen Sie Domänen aus der Liste der genehmigten Domänen

1. Wählen Sie eine oder mehrere Domänen in der Liste "Genehmigte vPro-Domänen" aus (mehrere Namen wählen Sie aus, indem Sie die STRG-Taste gedrückt halten und klicken).
2. Klicken Sie auf **Entfernen**.

Konfigurieren von vPro Remote Access

Intel vPro Remote Access ist eine Kombination aus Prozessortechnologien, Hardwareerweiterungen, Verwaltungsfunktionen und Sicherheitstechnologien, die einen Zugriff auf Intel vPro-aktivierte Geräte gestatten, wenn diese nicht mit Ihrem Unternehmensnetzwerk verbunden sind. Dieses Dialogfeld verwenden Sie, um den Remotezugriff auf Ihre Intel vPro-Geräte zu konfigurieren.

Intel vPro Gateway-Konfiguration

Diesen Abschnitt verwenden Sie zur Eingabe von Konfigurationsdaten zu dem Server, den Sie als vPro Gateway-Server verwenden.

- **vPro Gateway – interner Zugriff**: Dies ist die IP-Adresse des Servers, wenn der Zugriff intern, d. h. von innerhalb des Unternehmensnetzwerks erfolgt.
- **vPro Gateway – externer Zugriff**: Dies ist die IP-Adresse des Servers, wenn der Zugriff extern, d. h. von außerhalb des Unternehmensnetzwerks erfolgt.
- **vPro Gateway-HTTP-Port**: Dies ist der Port, der für die HTTP-Kommunikation zwischen dem Intel vPro Gateway-Server und dem Coreserver verwendet wird. (Standardport: 8080)
- **vPro Gateway-Umleitungsport**: Dies ist der Port, der für IDE-Umleitung verwendet wird. (Standardport: 16993)
- **vPro Gateway-Clientport**: Dies ist der Port, der für die Kommunikation zwischen dem verwalteten Client und dem Intel vPro Gateway-Server verwendet wird. (Standardport: 20015)

Konfiguration periodischer Sitzungen für den Remotezugriff

Diese Einstellungen legen fest, wie oft und für wie lange Remotezugriffssitzungen zur Durchführung von Wartungsarbeiten auf Intel vPro-Geräten automatisch geöffnet werden.

- **Sitzungsintervall**: Gibt die Anzahl der Stunden zwischen den Starts der einzelnen Remotesitzungen an. Der Standardwert ist 24 Stunden.
- **Sitzungsdauer**: Gibt die Anzahl der Minuten an, die eine Remotesitzung aktiv bleibt, bis sie automatisch geschlossen wird. Der Standardwert ist 30 Minuten, der Mindestwert ist 10 Minuten.

Clientkonfiguration für den Remotezugriff

Markieren Sie das Kontrollkästchen **Remotezugriff auf allen vPro-Clients aktivieren**, um alle Intel vPro-Geräte für Remotezugriff zu aktivieren, wenn die Geräte verwaltet werden. Wenn diese Option aktiviert ist, stellen die Geräte automatisch eine Verbindung her, wenn sie sich außerhalb des Netzwerks befinden. Wenn diese Option nicht ausgewählt ist, werden die Einstellungen für den Remotezugriff zwar in der Datenbank gespeichert, aber nicht per Push auf die verwalteten Intel vPro-Geräte verteilt.

Remote vPro-Sitzungen öffnen

Diese Abschnitt zeigt die derzeit geöffneten Remotesitzungen mit Intel vPro-Geräten an.

Um eine Sitzung sofort zu beenden, wählen Sie eine Sitzung in der Liste aus und klicken dann auf **Sitzung beenden**.

Um ein Intel vPro-Gerät remote zu starten, wählen Sie eine derzeit geöffnete Sitzung und klicken auf **vPro Boot-Manager**. Sie können das Gerät von CD oder DVD, der lokalen Festplatte, über PXE oder IDE-Umleitung starten.

Verwalten von Intel vPro-Geräten

Management Suite unterstützt Geräte, die Intel vPro-Technologie verwenden. Intel vPro ist eine Hardware- und Firmwaretechnologie, mit der sich Geräte und Sicherheit remote verwalten lassen. Intel vPro verwendet für den Zugriff auf Geräte Out-of-Band-Kommunikation (OOB), unabhängig vom Zustand des Betriebssystems oder der Stromversorgung des Geräts.

Bei diesem Produkt bezieht sich der Ausdruck "Intel vPro" auf Technologien, die auf Desktopcomputern und mobilen Computern mit Intel vPro-Unterstützung bereitgestellt werden. Dieses Produkt unterstützt ferner Geräte mit früheren Versionen von Intel Active Management-Technologie (Intel AMT). Das Verfahren der Geräteversorgung mit verschiedenen Versionen von Intel vPro ist je nach Versionsnummer verschieden.

Intel vPro-Geräteverwaltung

Nachdem ein Intel vPro-Gerät erkannt und der Coredatenbank hinzugefügt wurde (damit es verwaltet werden kann), kann das Gerät in eingeschränktem Umfang verwaltet werden, auch wenn kein LANDesk Agent auf dem Gerät installiert ist.

Solange Geräte mit dem Netzwerk verbunden und mit Standbystrom versorgt sind, können sie erkannt und zur Datenbank hinzugefügt werden, um mit anderen Geräten im Netzwerk verwaltet zu werden.

Falls auf einem Gerät zwar Intel vPro, aber kein Verwaltungsagent installiert ist, kann das Gerät erkannt, zur Inventardatenbank hinzugefügt und im Ordner "Geräte" der Netzwerkansicht angezeigt werden. Für mit Intel vPro konfigurierte Geräte stehen u.a. folgende Verwaltungsfunktionen zur Verfügung:

- **Inventarübersicht:** Ein Teilsatz der normalen Inventardaten kann abgerufen und in Echtzeit für das Gerät angezeigt werden, auch wenn das Gerät ausgeschaltet ist.
- **Ereignisprotokoll:** Ein Protokoll mit Intel vPro-spezifischen Ereignissen, das den Schweregrad und die Beschreibung der Ereignisse anzeigt, kann in Echtzeit dargestellt werden.
- **Remote Bootmanager:** Energiezyklus und mehrere Startoptionen können von der Remote-Verwaltungskonsole aus initiiert werden, unabhängig vom Betriebssystemzustand oder der Stromzufuhr des Geräts. Welche Optionen bereitgestellt werden, hängt davon ab, welche Optionen auf dem Gerät unterstützt werden. Einige Geräte unterstützen unter Umständen nicht alle Startoptionen.
- **System Defense**: Die Intel vPro System Defense-Funktion setzt Netzwerksicherheitsrichtlinien auf verwalteten Geräten durch.

Andere Verwaltungsoptionen von Management Suite werden nur bereitgestellt, wenn ein Verwaltungsagent auf dem Gerät installiert ist.

In der folgenden Tabelle werden die Verwaltungsoptionen aufgeführt, die einem Gerät zur Verfügung stehen, auf dem nur Intel vPro installiert ist, verglichen mit einem Gerät, das über Intel vPro und einen Management Suite Management Agent verfügt.

	Nur Intel vPro	Intel vPro und Agent	Nur Agent
Inventarübersicht	Übersicht	X	X
Ereignisprotokoll	X	X	X

	Nur Intel vPro	Intel vPro und Agent	Nur Agent
Remote-Bootmanager	X	X	
Inventarverlauf		X	X
Remotesteuerung		X	X
Chat		X	X
Dateiübertragung		X	X
Remoteausführung		X	X
Reaktivieren		X	X
Herunterfahren		X	X
Neustart		X	X
Inventarscan		X	X
Geplante Tasks und Richtlinien	beschränkt	X	X
Gruppenoptionen		X	X
Inventarbericht ausführen		X	X
Intel vPro Alarmierung		X	X
Erkennung der Netzwerkumgebung	X	X	
Vom Client initiierter Remotezugriff	X	X	

Zugreifen auf Geräte, die mit dem Enterprise-Modus bereitgestellt wurden

Wenn Sie ein Intel vPro-Gerät im Enterprise-Modus versorgen, installiert der Coreserver ein Zertifikat für die sichere Kommunikation auf dem Gerät. Wenn das Gerät von einem anderen Coreserver verwaltet werden soll, muss die Versorgung des Geräts rückgängig gemacht und das Gerät dann vom neuen Coreserver erneut versorgt werden. Andernfalls reagiert der Intel vPro-Zugang des Geräts nicht, weil der neue Coreserver nicht über ein übereinstimmendes Zertifikat verfügt. Gleichermaßen gilt, dass andere Computer, die versuchen, auf die Intel vPro-Funktionalität zuzugreifen, scheitern werden, da sie kein übereinstimmendes Zertifikat besitzen.

Intel vPro-Verwaltungsfunktionen

Wenn ein Intel vPro-Gerät zur Inventardatenbank hinzugefügt wurde, werden mehrere Verwaltungsfunktionen aktiviert. Zugriff auf diese Funktionen erhalten Sie, indem Sie in der Netzwerkansicht mit der rechten Maustaste auf das Gerät klicken und **Intel vPro-Optionen** auswählen.

Ob diese Funktionen aktiviert sind und in welchem Umfang bei ihrer Verwendung Daten ausgegeben werden, hängt davon ab, ob das Gerät versorgt wurde und ob eine aktive Verbindung zu dem Gerät besteht. Welche Daten angezeigt werden, hängt von der auf dem Gerät vorhandenen Intel vPro-Version ab.

Intel vPro-Status

Das Dialogfeld "Intel vPro-Status" zeigt aktuelle Informationen zu den Intel vPro-Funktionen an, die aktiviert wurden und für das Gerät gelten. Hierzu gehören allgemeine Informationen, Energieeinstellungen, Wirelessprofil, Agentenpräsenz, System Defense, Erkennung der Netzwerkumgebung und Einstellungen für den Remotezugriff.

Funktionen, die auf dem Gerät nicht unterstützt werden, sind abgeblendet.

So zeigen Sie die Intel vPro-Inventarübersicht eines Geräts an

1. Klicken Sie in der Netzwerkansicht mit der rechten Maustaste auf ein Intel vPro-Gerät.
2. Wählen Sie **Intel vPro-Optionen > Intel vPro-Status** aus.
3. Zum Aktualisieren der Informationen klicken Sie auf **Aktualisieren**.

Intel vPro-Ereignisprotokoll

Management Suite stellt eine Ansicht des Ereignisprotokolls bereit, das von den Intel vPro-Geräten generiert wird. Die Einstellungen bestimmen, welche Ereignisse in diesem Protokoll aufgezeichnet werden. Sie können das Datum/die Uhrzeit des Ereignisses, die Quelle des Ereignisses (Einheitsspalte), eine Beschreibung und den durch die Intel vPro-Einstellungen festgelegten Schweregrad (Kritisch oder Nicht-kritisch) anzeigen. Sie können außerdem die Protokolldaten in einem kommabegrenzten (CSV-)Format exportieren.

So zeigen Sie das Intel vPro-Ereignisprotokoll an

1. Klicken Sie mit der rechten Maustaste in der Netzwerkansicht auf ein Intel vPro-Gerät und wählen Sie **Intel vPro-Optionen > Intel vPro-Ereignisprotokoll** aus.
2. Um die Daten in eine durch Trennzeichen getrennte Datei (*.CSV) zu exportieren, klicken Sie auf die Schaltfläche **Exportieren** in der Symbolleiste und geben einen Dateinamen an.
3. Um alle Daten im Protokoll zu löschen, klicken Sie auf die Schaltfläche **Protokoll löschen** auf der Symbolleiste.
4. Zur Aktualisierung der Protokolleinträge klicken Sie auf die Schaltfläche **Aktualisieren** auf der Symbolleiste.

Rollup-Cores

Installieren eines Rollup-Cores

Sie können einen Rollup-Core verwenden, um die Daten mehrerer Coreserver miteinander zu kombinieren. Sie müssen Rollup-Core-Aktualisierungen planen, um die Rollup-Coredatenbank mit der Coredatenbank eines jeden Coreservers zu synchronisieren. Über die Management Suite Webkonsole können Sie dann Geräte im Rollup-Core mithilfe von Abfragen und unter Verwendung der Softwareverteilung, der Remotesteuerung und anderer Funktionen, die von der Webkonsole unterstützt werden, verwalten.

Bevor Sie einen Rollup-Core installieren, müssen Sie einen zusätzlichen Rollup-Datenbankserver für Oracle- oder SQL Server konfigurieren. Die Management Suite Setup Rollup-Option fordert Sie zur Eingabe von Informationen zu der von Ihnen eingerichteten Datenbank auf.

Sie können mit einem Rollup Daten aus Cores zusammenführen, die Management Suite Version 8.7 SP2 oder eine höhere Version verwenden. Der Rollup-Core muss von der neuesten Management Suite Version aus installiert werden. Alle Cores müssen denselben Datenbanktyp verwenden, also nur SQL oder nur Oracle. Wenn Sie einen Rollup für Daten aus älteren Versionen als Management Suite Version 9.0 durchführen, und Sie außerdem eine Doppelbyteversion von Management Suite (Japanisch, Chinesisch oder Russisch) verwenden, dann müssen alle Cores dieselbe Sprache verwenden.

So installieren Sie einen Rollup-Core

1. Richten Sie einen Server als Host für den Rollup-Core und die Datenbank ein.
2. Installieren Sie die Datenbank auf dieselbe Weise wie bei einer normalen Management Suite Installation. Weitere Informationen zur Installation der Datenbank finden Sie auf der Website der LANDesk Community unter http://community.landesk.com.
3. Melden Sie sich beim Rollup-Coreserver mit einem Konto an, das über Administratorrechte verfügt.
4. Installieren Sie den Rollup-Core über die Autorun-Funktion auf Ihrem Management Suite-Installationsdatenträger (oder Beenden Sie das Setup.

Konfigurieren von Rollup-Datenbanklinks

In diesem Abschnitt wird beschrieben, wie Datenbanklinks auf Rollup-Cores konfiguriert werden. Dieser Schritt muss ausgeführt werden, bevor mit dem Rollup von Daten begonnen werden kann.

Die mit dieser Konfiguration beauftragte Person benötigt darüber hinaus Zugriff auf alle von LANDesk verwendeten Datenbankverwaltungssysteme (DBMS) und muss Sicherheitsberechtigungen zum Erstellen von Datenbanklinks und Ausführen von Konfigurationsschritten auf DBMS-Serverebene besitzen.

Oracle-Rollup auf Oracle

So konfigurieren Sie die Oracle-Datenbank

Die Datei "TNSNames.ora" auf dem Datenbankserver, in dem sich Ihre Rollup-Datenbank befindet, muss einen Eintrag für Ihre Coreserver-Datenbank enthalten.

1. Melden Sie sich für eine Oracle-Datenbank innerhalb der Enterprise Manager Console bei Ihrer Datenbank an. Erweitern Sie **Verteilt**.
2. Klicken Sie mit der rechten Maustaste auf das Element **Datenbanklinks** und dann auf **Erstellen**.

3. Geben Sie im Feld **Name** einen Namen für Ihren Datenbanklink ein.
   Hinweis: Wenn die AR-Datenbank Oracle9i verwendet, ist als Linkname jeder noch nicht benutzte oder reservierte Name zulässig. Das Installationsprogramm fordert Sie zur Eingabe dieser Informationen auf.
4. Wählen Sie **Fester Benutzer** aus und geben Sie einen Benutzernamen und ein Kennwort für die Datenbank des Coreservers ein.
5. Geben Sie in das Feld **Dienstname** den TNSNames.ora-Eintrag (d. h. NetAlias) ein, der auf Ihre Coreserver-Datenbank verweist.
6. Klicken Sie auf **Erstellen**.
7. Doppelklicken Sie auf Ihren neu erstellten Link und klicken Sie auf **Testen**. Sie sollten eine Nachricht erhalten, die bestätigt, dass der Link aktiv ist. Sie können Ihren Link außerdem testen, indem Sie sich bei der Rollup-Datenbank anmelden und folgenden Befehl eingeben:
   Select count(*) from computer@linkname;
   Wenn daraufhin eine Aufzählung der Geräte in der Produktionsdatenbank des Coreservers zurückgegeben wird, so bedeutet dies, dass der Link ordnungsgemäß konfiguriert wurde.

SQL Server-Rollup auf SQL Server

So konfigurieren Sie die SQL Server-Datenbank

1. Öffnen Sie SQL Server Management Studio.
2. Erweitern Sie sowohl Ihren Server als auch **Serverobjekte**.
3. Klicken Sie mit der rechten Maustaste auf das Element **Verbindungsserver** und dann auf **Neuer Verbindungsserver**.
4. Führen Sie auf der Seite **Allgemein** die Schritte 5 – 11 aus:
5. **Verbindungsserver**: Geben Sie einen eindeutigen Namen für diesen Datenbanklink ein (z. B. LDMS core server1-Link).
6. Wählen Sie **Andere Datenquelle** aus.
7. Wählen Sie **Microsoft OLE DB Provider für SQL Server** aus.
8. **Produktname**: Geben Sie LDMS ein.
9. **Datenquelle**: Geben Sie den Namen des Datenbankservers ein, auf dem sich die Coredatenbank befindet.
10. **Providerzeichenfolge** bzw. Anbieterzeichenfolge: Geben Sie die Zeichenfolge des Providers ein. Zum Beispiel:

    SQL Server
    provider=SQLOLEDB.1;user id=<Benutzer für die Datenbank des Coreservers>
    *** Der Abschnitt "user id" der Provider-Zeichenfolge wird im Connection-String für die Verbindung mit einer anderen SQL Server-Datenbank benötigt. ***

11. **Katalog**: Geben Sie den physikalischen Namen der Datenbank Ihres Coreservers ein (z. B. lddb).
12. Wählen Sie auf der Seite **Sicherheit** die Option **In folgendem Sicherheitskontext verwendet** aus, geben Sie den Benutzernamen und das Kennwort für die Datenbank des Coreservers ein und klicken Sie dann auf **OK**.

13. Klicken Sie auf **Neue Abfrage** und geben Sie den folgenden Befehl ein:
    Select count(*) from [Linkname].[Datenbankname].[Name des Tabelleneigentümers].Computer
    Bei Verwendung der obigen Werte würde diese Abfrage wie folgt angezeigt:
    Select count(*) from [LDMS Coreserver1-Link].[lddb].[dbo].Computer
    Wenn die korrekte Anzahl zurückgegeben wird, wurde der Link ordnungsgemäß eingerichtet.

Verwenden des Datenbank-Rollup-Dienstprogramm

Mithilfe des Datenbank-Rollup-Dienstprogramms (DBRollup.exe) können Sie mehrere Quell-Coredatenbanken zu einer einzigen Core-Rollup-Zieldatenbank zusammenfassen. Der Grenzwert des Rollup-Core-Geräts hängt von Ihrer Hardware und den akzeptablen Leistungsniveaus ab. Die Quelldatenbank kann entweder ein Coreserver oder ein Rollup-Coreserver sein.

Die Systemanforderungen für eine Zieldatenbank können erheblich höher sein als die für eine Standarddatenbank. Diese Anforderungen können je nach Netzwerkumgebung stark variieren. Wenn Sie weitere Informationen zu den Hardware- und Softwareanforderungen für Ihre Zieldatenbank benötigen, wenden Sie sich an den LANDesk Software-Support.

Das Setup installiert das Datenbank-Rollup-Dienstprogramm automatisch mit dem Rollup-Core. Das Rollup-Dienstprogramm verwendet einen Pullprozedur für den Zugriff auf Daten auf den von Ihnen ausgewählten Cores. Damit Datenbank-Rollups funktionieren, muss bereits jedem Core, von dem das Rollup-Dienstprogramm Daten abrufen soll, ein Laufwerk zugeordnet sein. Das Konto, zu dem Sie eine Verbindung herstellen, muss über Leserechte für die Registrierung des Coreservers verfügen.

Das Rollup-Tool sucht anhand eines Registrierungsschlüssels auf dem Coreserver nach Datenbank- und Verbindungsdaten (HKLM\SOFTWARE\LANDesk\ManagementSuite\Core\Connections\local) und verwendet die Daten dieses Schlüssels, um auf die Datenbank zuzugreifen, die mit dem jeweiligen Core, den Sie zum Rollup-Tool hinzufügen, verknüpft ist. Bei Oracle-Datenbanken muss die TNS-Definition auf dem Server, auf dem Sie das Rollup-Dienstprogramm ausführen, der TNS-Definition auf dem Coreserver entsprechen, auf den das Dienstprogramm zugreift.

Sie können das Rollup-Tool verwenden, um die Attribute auszuwählen, für die ein Rollup von den Cores durchgeführt werden soll. Die von Ihnen ausgewählten Attribute gelten für alle Cores. Durch Verringern der Attributzahl wird die Rollup-Zeit und die während den Rollups übertragene Datenmenge reduziert. Wenn Sie wissen, dass Sie keine Abfragen nach gewissen Attributen durchführen, können Sie diese entfernen.

Das Rollup-Tool führt immer einen Rollup der ausgewählten Attributdaten durch. Das Rollup-Dienstprogramm bezieht auch keine von Ihnen definierten Abfragen oder Bereiche ein. Alle Konsolenbenutzer mit Rechten für die Rollup-Datenbank haben auf alle Daten in dieser Datenbank Zugriff. Sie können die Sicherheit auf Funktionsebene verwenden, um den Zugriff auf Webkonsolenfunktionen einzuschränken.

Nachdem Sie die Coreserver für den Rollup und die Attributliste für diese Server hinzugefügt haben, können Sie auf **Planen** klicken, um das Skript für einen geplanten Rollup für jeden Coreserver hinzuzufügen. Von einer Webkonsole können Sie diese Rollup-Skripte so planen, dass sie zum gewünschten Zeitpunkt und im gewünschten Intervall ausgeführt werden. Rollup-Skripte werden nur auf der Webkonsole angezeigt und sind auf dem Rollup-Core resident.

Starten des Rollup-Dienstprogramms

So starten Sie das Rollup-Dienstprogramm

1. Führen Sie auf einem Rollup-Core das Rollup-Tool aus (\Programme\LANDesk\ManagementSuite\dbrollup.exe).
2. Wählen Sie einen zu verwaltenden, bereits vorhandenen Rollup-Coreserver aus der Liste aus, oder klicken Sie auf **Neu**, um den Namen eines neuen Rollup-Coreservers einzugeben. Achten Sie darauf, dass Sie den Namen des Coreservers eingeben, nicht den der Datenbank.
3. Sobald Sie einen Rollup-Core ausgewählt haben, werden in der Liste der **Quell-Cores** die Cores angezeigt, die Sie für den Rollup auf den ausgewählten Rollup-Core konfiguriert haben.

Informationen zum Rollup-Dienstprogramm

Verwenden Sie das Datenbank-Rollup-Dienstprogramm (auszuführen vom Rollup-Core), um Daten-Rollups von Coreservern zu verwalten.

- **Rollup-Core:** Sie können mehrere Rollup-Cores über das Rollup-Dienstprogramm verwalten. Wählen Sie den Core aus, den Sie verwalten möchten. Zunächst müssen Sie ein Laufwerk für jeden Rollup-Core zuordnen.
- **Neu:** Klicken Sie auf "Neu", um einen neuen Rollup-Core hinzuzufügen, den Sie verwalten möchten. Zunächst müssen Sie ein Laufwerk für jeden hinzuzufügenden Rollup-Core zuordnen. Geben Sie den Computernamen des Rollup-Core ein und klicken Sie auf **OK**.
- **Attribute:** Wählen Sie per Mausklick die Attribute aus, für die ein Rollup durchgeführt werden soll. Die Attributliste gilt global für alle Coreserver, die der ausgewählte Rollup-Core verwendet. Verschieben Sie einzelne Attribute oder Attributstrukturen aus der Spalte "Ausgewählte Attribute" (für diese Attribute wird ein Rollup durchgeführt) in die Spalte "Verfügbare Attribute" (für diese Attribute wird kein Rollup durchgeführt).
- **Datenbank zurücksetzen:** Klicken Sie auf "Datenbank zurücksetzen", um die ausgewählte Rollup-Datenbank zurückzusetzen. Sämtliche Daten werden hierdurch gelöscht und alle Tabellen neu aufgebaut.
- **Hinzufügen:** Klicken Sie auf "Hinzufügen", um einen Core hinzuzufügen, dessen Daten im ausgewählten Rollup-Core enthalten sein sollen.
- **Löschen:** Klicken Sie auf "Löschen", um den ausgewählten Core und dessen Daten aus der Datenbank des Rollup-Cores zu entfernen. **WARNUNG:** Mit dieser Option werden die Daten des ausgewählten Core gelöscht, sobald Sie auf **OK** klicken. Daten von anderen Coreservern bleiben in der Rollup-Datenbank gespeichert.
- **Planen:** Klicken Sie auf "Planen", um ein Rollup-Skript für den ausgewählten Core hinzuzufügen. Wenn Sie im Feld "Quellcores" keinen Core ausgewählt haben, erstellt diese Option Rollup-Skripte für alle Cores im Feld "Quellcores".
- **Rollup:** Klicken Sie auf "Rollup", damit der ausgewählte Core umgehend ein Rollup ausführt. Es muss ein Core ausgewählt sein, damit diese Option zur Verfügung steht.
- **Schließen:** Klicken Sie auf "Schließen", um das Rollup-Dienstprogramm zu schließen.

Konfigurieren von Attributen, für ein Rollup durchgeführt werden soll

So konfigurieren Sie die Attribute, für die ein Rollup durchgeführt werden soll

1. Wählen Sie über das Rollup-Dienstprogramm den Rollup-Core aus, den Sie konfigurieren möchten.
2. Klicken Sie auf **Attribute**.
3. Standardmäßig wird für alle Datenbankattribute ein Rollup durchgeführt. Verschieben Sie die Attribute, für die kein Rollup durchgeführt werden soll, von der Spalte **Ausgewählte Attribute** in die Spalte **Verfügbare Attribute**.
4. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben. Wenn Attribute in die Spalte "Verfügbare Attribute" verschoben werden, werden verknüpfte Daten aus der Rollup-Datenbank gelöscht.

Konfigurieren der Quell-Coreserver für einen Rollup-Core

So konfigurieren Sie die Quell-Coreserver für einen Rollup-Core

1. Wählen Sie über das Rollup-Dienstprogramm den Rollup-Core aus, den Sie konfigurieren möchten.
2. Sobald Sie einen Rollup-Core ausgewählt haben, werden in der Liste der Quellcores die Cores angezeigt, die Sie für das Rollup auf dem ausgewählten Rollup-Core konfiguriert haben. Klicken Sie auf **Hinzufügen**, um weitere Cores hinzuzufügen, oder wählen Sie einen Core aus und klicken Sie auf **Löschen**, um einen Core zu löschen.

WARNUNG: Sobald Sie auf **Löschen** klicken, wird der ausgewählte Core einschließlich aller Daten, die zu diesem Core gehören, aus der Rollup-Coredatenbank gelöscht. Wenn Sie beim Hinzufügen eines Coreservers zur Rollup-Datenbank einen ungültigen Linknamen bereitstellen, müssen Sie zudem den Core aus dem Rollup entfernen und erneut hinzufügen, um den Linknamen zu ändern.

Planen von Datenbank-Rollup-Jobs

Es kann immer nur ein Rollup abgearbeitet werden. Ein geplanter Rollup misslingt, wenn bereits ein anderer Rollup abgearbeitet wird. Sorgen Sie dafür, dass durch genügend zeitlichen Abstand zwischen den Rollups Überlappungen vermieden werden. Wenn sich schwer abschätzen lässt, zu welchem Zeitpunkt Rollups stattfinden, empfiehlt es sich, die Rollups als Einzelaufträge zu planen. Wählen Sie hierzu mehrere Cores aus, bevor Sie auf **Planen** klicken. Auf diese Weise werden die Rollups automatisch einzeln abgearbeitet.

WARNUNG: Achten Sie darauf, Rollups nicht für solche Zeiten einzuplanen, zu denen die Cores Downloads für Patchinformationen durchführen. Der Download von Patchinformationen stellt eine große Belastung für die Datenbank dar und verlangsamt den Rollup erheblich.

So werden Datenbank-Rollup-Jobs auf der Webkonsole geplant

1. Wählen Sie im Rollup-Dienstprogramm den **Rollup-Core** aus, den Sie konfigurieren möchten.
2. Wählen Sie in der Liste **Quellcores** die Cores aus, für die Sie ein Rollup planen möchten, und klicken Sie auf **Planen**. Wenn Sie keine Cores auswählen, werden alle Cores in der Liste standardmäßig eingeplant, sobald Sie auf **Planen** klicken. Wenn Sie auf **Planen** klicken, wird ein Rollup-Skript für den ausgewählten Core dem ausgewählten Rollup-Core hinzugefügt. Wenn Sie mehrere Cores auswählen, werden diese als ein Auftrag geplant und nacheinander verarbeitet.
3. Stellen Sie von einer Webkonsole eine Verbindung zum Rollup-Coreserver her.
4. Klicken Sie im linken Navigationsfenster auf **Planen von Rollup-Jobs**.
5. Klicken Sie auf das Rollup-Skript, für das Sie eine Planung durchführen möchten. Die Skriptnamen beginnen mit dem Namen des Quellcores, gefolgt vom Namen des Ziel-Rollup-Cores in Klammern. Klicken Sie auf **Rollup planen**.
6. Wählen Sie aus, wann der Rollup durchgeführt und ob er automatisch neu geplant werden soll. Achten Sie darauf, dass kein Rollup für mehr als einen Core gleichzeitig ausgeführt wird. Klicken Sie auf **Mit dem nächsten Schritt fortfahren**.
7. Prüfen Sie den Skriptplan und klicken Sie auf **Fertig stellen**.

HINWEIS: Nach dem Rollup von Daten, die von Coreservern stammen, auf denen eine ältere Version als Management Suite Version 9.0 ausgeführt wird, zeigt das Dialogfeld **Rollup-Status** der Datei der DBRollup.exe Folgendes an: "Task mit einem oder mehreren Fehlern abgeschlossen". Dies ist normal. Wenn Sie einen Rollup-Task für einen Core mit einer älteren Version als 9.0 planen, zeigt darüber hinaus der Status des geplanten Tasks auch bei erfolgreichem Abschluss des Tasks die Meldung "Fehlgeschlagen - Task Handler hat einen Fehler entdeckt" an. Auch das ist normal. Sie sollten aber die DBRollup- und Datenbankprotokolle kontrollieren, falls Sie irgendeine andere Fehlerursache vermuten, wie beispielsweise eine Datenbanksperre.

Replizieren von Rollup-Core-Daten auf Quellcores

Wenn in Ihrer LANDesk Umgebung ein Rollup-Core installiert ist, können Sie Folgendes auf Quell-Coreserver replizieren:

- Abfragen
- Verteilungspaketkonfigurationen
- Konfigurationen für Verteilungsmethoden

Sie können Standardkonfigurationen für diese Elemente auf dem Rollup-Core erstellen und sie dann mithilfe der Replizierungsfunktion für Ihre Management Suite Benutzer auf Quellcores zur Verfügung stellen.

Das Tool **Auf Cores replizieren** wird angezeigt, wenn die Webkonsole mit einem Rollup-Core verbunden ist. Das von Ihnen zum Herstellen der Verbindung verwendete Konto muss ein LANDesk Administrator-Konto sein. Wenn Sie auf dieses Tool klicken, wird ein Dialogfeld angezeigt, in das Sie den Namen des Replizierungstasks eingeben und das zu replizierende Objekt auswählen können. Wenn Sie diese Informationen konfigurieren und auf **OK** klicken, wird ein Task mit dem von Ihnen ausgewählten Namen in der Ansicht **Geplante Tasks** des Rollup-Cores zur Verfügung gestellt.

Die Replizierung erfolgt erst, nachdem Sie den Replizierungstask für die Ausführung konfiguriert haben. Sie können den Task manuell mithilfe der Option **Jetzt starten** ausführen, oder Sie können einen sich wiederholenden Ausführungsplan für den Task erstellen. Während der Ausführung des Task erstellt der Rollup-Core ein XML-Dokument mit den zu replizierenden Informationen. Replizierungstasks sind weder umfassend noch anspruchsvoll, sodass Sie jeden beliebigen Replizierungsplan verwenden können, der von Ihrer Verwaltungsumgebung unterstützt wird.

Replizierungstasks verwenden keine manuell ausgewählten Ziele. Quellcores mit einem Rollup-Core-Zertifikat erhalten die XML-Datei und zeigen dann die replizierten Daten an. Wenn Sie Rollup-Core-Zertifikate anfügen möchten, können Sie dazu das Datenbank-Rollup-Dienstprogramm (DBRollup.exe) verwenden.

Nur Daten mit dem Eigentümer "Öffentlich" werden repliziert. Wenn Sie Daten nicht replizieren möchten, ordnen Sie sie einem anderem Eigentümer als "Öffentlich" zu. Replizierte Daten auf Quellcores können bearbeitet werden; um jedoch zu verhindern, dass Ihre Änderungen überschrieben werden, wenn die nächste Replizierung für ein Element mit demselben Namen erfolgt, müssen Sie den Namen des Elements ändern. Wenn sich replizierte Elemente in benutzerdefinierten Gruppen auf dem Rollup-Core befinden, wird die Gruppenstruktur ebenfalls auf die Quellcores repliziert.

Beim Replizieren werden nur die replizierten Daten den Quellcores hinzugefügt. Wenn Sie ein Element auf dem Rollup-Core löschen, das zu einem bestimmten Zeitpunkt repliziert worden war, so wird diese Löschung auf den Quellcores nicht durchgeführt. Wenn Sie ein repliziertes Element auf Quellcores löschen möchten, müssen Sie dies manuell tun.

So verwenden Sie die Replizierung auf einem Rollup-Core

1. Konfigurieren Sie auf dem Rollup-Core die öffentlichen Abfragen, Verteilungspakete und Verteilungsmethoden, die Sie replizieren möchten.
2. Klicken Sie, sobald Sie mit der Webkonsole des Rollup-Cores über ein LANDesk Administrator-Konto verbunden sind, auf das Tool **Auf Cores replizieren**.
3. Geben Sie einen Tasknamen ein und aktivieren Sie die Kontrollkästchen der zu replizierenden Elemente.
4. Klicken Sie auf **OK**.
5. Klicken Sie auf das Tool **Geplante Tasks**.
6. Starten Sie jetzt den Replizierungstask oder konfigurieren Sie einen Zeitplan für die Taskausführung. Wenn der Task ausgeführt wird, werden die replizierten Daten an Quell-Coreserver, die über ein Rollup-Core-Zertifikat verfügen, übertragen.

Erhöhen des Timeoutwerts für die Rollup-Datenbank

Bei großen Rollup-Datenbanken meldet der Abfrageeditor der Webkonsole möglicherweise einen Timeout (Zeitüberschreitungsfehler), wenn er versucht, eine lange Liste anzuzeigen (z. B. die Liste mit den Namen der Softwarepakete). Wenn dies der Fall ist, enthält die Liste, die Sie anzeigen möchten, keine Daten. Wenn es zu Timeouts kommt, müssen Sie den Timeoutwert für die Datenbank heraufsetzen. Der Wert muss überall geändert werden, wo der IIS-Dienst oder der Webkonsolenserver installiert wird. Fügen Sie unter dem Registrierungsschlüssel

- HKEY_LOCAL_MACHINE\SOFTWARE\LANDesk\ManagementSuite\Core

Fügen Sie ein neues DWORD, Timeout, mit einem Dezimalwert von 1800 hinzu. Dieser Wert wird in Sekunden angegeben. Sie können diesen Wert nach Bedarf an die von Ihnen verwendeten Abfragetypen und an die Datenbankleistung anpassen. Stoppen Sie IIS und starten Sie ihn neu, damit die Änderungen übernommen werden.

Bevorzugte Server und Inhaltsreplikation

Bevorzugte Server und Inhaltsreplikation – Übersicht

Mit der Verwendung von bevorzugten Servern reduziert Management Suite die Netzwerkbelastung bei der Verteilung über die Subnetze. Im Anschluss an die ordnungsgemäße Konfiguration werden bevorzugte Server in die Reihenfolge einbezogen, in der Verteilungsziele nach Verteilungsdateien suchen:

1. Der lokale Verteilungscache des Ziels.
2. Lokale Peers im selben Subnetz wie das Ziel, in deren Verteilungscache sich Quelldateien befinden.
3. Falls konfiguriert, der nächste bevorzugte Server.
4. Die Verteilungsquelle, die ursprünglich im Verteilungspaket definiert war.

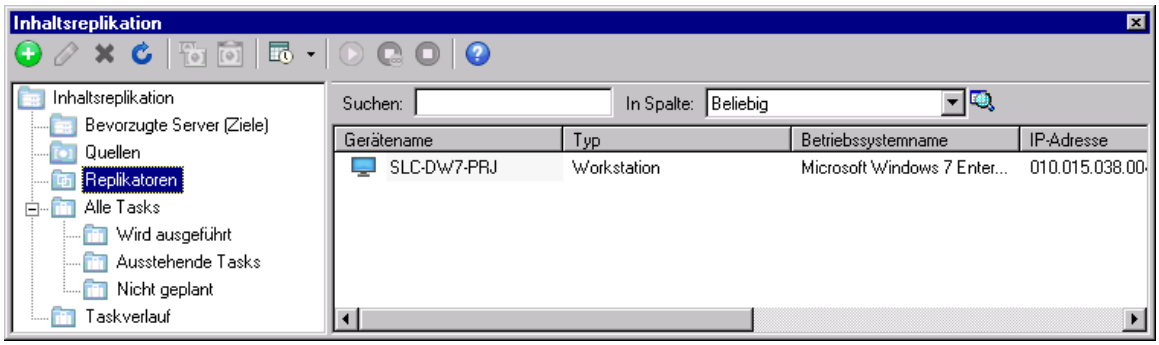
Die Inhaltsreplikation bietet eine Verwaltungsstruktur für die Einrichtung, die Synchronisierung und die Aktualisierung von Dateien auf bevorzugten Servern mit den Dateien, die sich auf einem Quellserver befinden. Sie müssen die Inhaltsreplikation nicht in Verbindung mit Ihren bevorzugten Servern verwenden, aber der Einsatz der Inhaltsreplikation gibt Administratoren ein einfaches Verfahren an die Hand, mit dem sie sicherstellen können, dass die Dateien auf den bevorzugten Servern innerhalb der gesamten IT-Umgebung nach einem vorgegebenen Zeitplan aktualisiert werden.

Für die Inhaltsreplikation müssen die folgenden Elemente konfiguriert werden:

- **Bevorzugter Server:** Dies ist der Server, von dem Verteilungsziele versuchen, Quelldateien herunterzuladen. Mit der Softwareverteilung kann zwar auf Dateien auf bevorzugten Servern zugegriffen werden, die nicht repliziert wurden, aber die Inhaltsreplikation ist die bessere Lösung, wenn es darum geht, diese Dateien stets auf dem neuesten Stand zu halten.
- **Quelle:** Dies ist der Server, auf dem sich die Dateien befinden, die auf bevorzugte Server repliziert werden müssen. Administratoren richten die Dateistrukturen und Dateien auf der Quelle ein und verwenden dann die Inhaltsreplikation, um diese Hierarchien auf bevorzugte Server zu kopieren.
- **Replikator:** Hierbei handelt es sich um ein verwaltetes Windows-Gerät, das Dateien von einer Quelle auf einen bevorzugten Server kopiert. Auf dem verwalteten Gerät sollte hinreichend Speicherplatz vorhanden sein, damit die Daten von allen Quellen im lokalen Cache gespeichert werden können. Wenn ein für die Replikation verwendetes verwaltetes Gerät nicht genügend Speicherplatz besitzt, muss der Replikator unter Umständen bei jedem Replikationstask einige Dateien von der Quelle herunterladen.

Replikatoren können nur Inhalte von einem Quellserver auf einen bevorzugten Server replizieren. Bei den replizierten Daten muss es sich nicht ausschließlich um Softwareverteilungsdaten handeln, solange es Sie nicht stört, dass sich diese Daten auf einem bevorzugten Server befinden. Sie können beispielsweise auch Dokumente und Kalkulationstabellen auf bevorzugte Server in remoten Niederlassungen replizieren.

Sie können eine beliebige Anzahl von bevorzugten Servern, Quellen und Replikatoren einrichten.



Konfigurieren von bevorzugten Servern

Sie können den Server angeben, der von Geräten bevorzugt auf Softwareverteilungspakete durchsucht wird. Dies kann in langsamen WAN-Umgebungen, in denen Geräte keine Pakete von Offsite-Servern herunterladen sollen, von Bedeutung sein. Wenn Sie bevorzugte Server angeben, können Sie auch die Nachweise angeben, die verwaltete Geräte verwenden sollten, um sich bei allen bevorzugten Servern zu authentifizieren. Sie können auch die IP-Adressbereiche angeben, für die der bevorzugte Server verfügbar ist.

Wenn Sie bevorzugte Server mit einem Verteilungsauftrag verwenden, wird nur der Serverteil des UNC- oder URL-Datei-/Paketpfads ersetzt; der Rest des Pfads muss mit der Angabe im Verteilungsauftrag übereinstimmen. Wenn sich die Datei nicht auf dem bevorzugten Server befindet, wird sie aus dem im Verteilungspaket angegebenen Speicherort heruntergeladen. Die einzige Verteilungsmethode, die bevorzugte Server nicht unterstützt, ist Multicast (nur Cache). Das UNC-Paket teilt sich die Arbeit mit allen Paketen. Das HTTP-Paket teilt sich die Arbeit nur mit MSI- und SWD-Paketen.

Der Coreserver verwendet Verteilungspakethashes zur Überprüfung von Verteilungspaketen in geplanten Tasks. Der Coreserver versucht zuerst, diese Hashes von einem bevorzugten Server her zu erzeugen, falls verfügbar. Die Verwendung eines lokalen bevorzugten Servers beschleunigt den Hashing-Vorgang bedeutend. Falls das Paket auf einem der bevorzugten Server nicht vorhanden ist, erzeugt der Coreserver das Pakethash vom Pfad her, der im Verteilungspaket angegeben ist. Im Allgemeinen empfiehlt es sich nicht, den Coreserver zum Hashing ein großes Paket über die WAN-Verbindung abrufen zu lassen; das Hashen von Dateien auf einem lokalen Server des Cores ist bedeutend schneller und beansprucht weniger Bandbreite.

Verwaltete Geräte speichern die Liste bevorzugter Server lokal in der Datei preferredserver.dat. Um diese Datei zu erstellen, kommuniziert ein Gerät mit dem Coreserver und macht dann eine gefilterte Liste bevorzugter Server (basierend auf IP-Adressbereicheinschränkungen, falls es solche gibt). Dann führt das Gerät eine Bandbreitenprüfung auf jedem bevorzugten Server durch und speichert die ersten drei Server in der Datei preferredserver.dat. Die Bandbreitenprüfung produziert jedoch keine garantiert zuverlässigen Ergebnisse. Beispiel: Ein Server, der in der Nähe steht, ist zur Zeit der Prüfung durch den Agenten vielleicht stark belastet und landet daher nicht auf der Liste, auch wenn er sonst der beste Kandidat wäre.

Der Verteilungsagent aktualisiert die Datei "preferredserver.dat" alle 24 Stunden oder wenn die IP-Adresse sich ändert. Nicht jedes Gerät muss diesen Vorgang durchführen. Geräte teilen ihre Liste bevorzugter Server mit Peers. Dies ist der Vorgang, den verwaltete Geräte ausführen, um eine aktuelle Liste bevorzugter Server zu erhalten:

1. Falls "preferredserver.dat" sich im lokalen Datei-Cache befindet, verwendet es der Verteilungsagenten.
2. Falls preferredserver.dat sich auf einem Peer befindet, ruft der Agent die Datei von diesem Peer ab.

3. Falls "preferredserver.dat" weder lokal noch auf einem Peer verfügbar ist, nimmt das Gerät Kontakt mit dem Coreserver auf, erstellt eine gefilterte Liste bevorzugter Server und speichert sie lokal als "preferredserver.dat".
4. Falls "preferredserver.dat" leer ist oder keiner der bevorzugten Server antwortet, sucht der Agent in der lokalen Registrierung nach einer Liste bevorzugter Server.

Wenn keiner dieser Schritte einen verfügbaren bevorzugten Server produziert, verwendet der lokale Agent den Verteilungspfad, der im Verteilungsauftrag angegeben ist.

Konfigurieren von bevorzugten Servern

Sie können den Server angeben, der von Geräten bevorzugt auf Softwareverteilungspakete durchsucht wird. Dies kann in langsamen WAN-Umgebungen, in denen Geräte keine Pakete von Offsite-Servern herunterladen sollen, von Bedeutung sein. Wenn Sie bevorzugte Server angeben, können Sie auch die Nachweise angeben, die verwaltete Geräte verwenden sollten, um sich bei allen bevorzugten Servern zu authentifizieren. Sie können auch die IP-Adressbereiche angeben, für die der bevorzugte Server verfügbar ist.

So konfigurieren Sie bevorzugte Server

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie in der Baumstruktur **Inhaltsreplikation** mit der rechten Maustaste auf **Bevorzugte Server (Ziele)** und klicken Sie dann auf **Neuer bevorzugter Server**.
3. Geben Sie auf der Seite "Konfiguration" die Serverinformationen und die Anmeldeinformationen für eine schreibgeschützte Verbindung ein. Klicken Sie auf **Anmeldeinformationen testen**, um sicherzustellen, dass die eingegebenen Anmeldeinformationen gültig sind.
4. Geben Sie auf der Seite für die IP-Adressbereiche die IP-Adressbereiche ein, die für diesen bevorzugten Server zulässig sein sollen.
5. Legen Sie auf den Seiten **Ausgewählter Replikator** den Replikator, die Ausführungsoptionen und den Zeitplan fest. Wenn Sie weitere Informationen benötigen, klicken Sie auf der jeweiligen Seite auf **Hilfe**.
6. Wählen Sie auf der Seite **Quellen** die Quellpfade, die repliziert werden sollen.
7. Geben Sie auf der Seite **Anmeldeinformationen für das Schreiben** die Anmeldeinformationen ein, die der Replikator zum Schreiben replizierter Dateien auf die als Ziel definierten bevorzugten Server verwenden soll. Klicken Sie auf **Anmeldeinformationen testen**, um sicherzustellen, dass die eingegebenen Anmeldeinformationen gültig sind.
8. Klicken Sie auf **Speichern**.

Speichern bevorzugter Paketserver in der Registrierung

Wenn Sie eine Fallback-Liste bevorzugter Server konfigurieren möchten, die verwendet wird, wenn in der Datei "preferredserver.dat" keine Server vorhanden sind, können Sie den folgenden Registrierschlüssel auf verwalteten Geräten erstellen und den Wert auf den Namen des bevorzugten Paketservers einstellen. Sie können mehrere Paketserver angeben, indem Sie sie durch Semikolons voneinander trennen.

- HKEY_LOCAL_MACHINE\Software\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\PreferredPackageServer

Beispieleintrag in der Registrierung:

- [HKEY_LOCAL_
  MACHINE\SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution]
  "PreferredPackageServer "="Server1;Server2;Server3"

Anpassen der in preferredserver.dat gespeicherten Serveranzahl

Standardmäßig enthält die Datei preferredserver.dat drei Server, dessen Testergebnisse zur Zeit der Bandbreitenprüfung die höchste Bandbreite angegeben haben. Sie können die Anzahl der in "preferredserver.dat" gespeicherten Dateien ändern, indem Sie diese Zeile in der Datei "ntstacfg.in#" im Ordner ldlogon des Coreservers aktualisieren. Gültige Werte liegen zwischen 0 und 7. Wenn Sie diese Datei aktiviert haben, werden die Änderungen Teil von neuen oder aktualisierten Agentenkonfigurationen. Sie müssen Ihre Agentenkonfiguration erneut an Geräte verteilen, damit die Änderung in Kraft tritt.

```
; Einstellungen für die Dateien lddwnld/ldredirect, DynamicPreferredServers ist die
; Höchstzahl bevorzugter Server, die gespeichert werden. Stellen Sie diesen Wert auf 0 ein
; um die Funktionalität des dynamischen bevorzugten Servers zu deaktivieren.
REG51=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\DynamicPreferredServers, 3, , REG_DWORD
```

Anpassen der Priorisierung bevorzugter Server

Um Verzögerungen zu vermeiden, wenn die meisten bevorzugten Server kein Paket haben, wird die Umleitungslogik anfangen, Server zu bevorzugen, die dem Gerät tatsächlich Dateien bereitgestellt haben. Sie können die Priorisierung der bevorzugten Server in "preferredserver.dat" ändern, indem Sie diese Zeilen in der Datei "ntstacfg.in#" im Ordner ldlogon des Coreservers aktualisieren.

```
; Um Verzögerungen zu vermeiden, wenn die meisten bevorzugten Server kein Paket haben
; wird die Umleitungslogik anfangen, Server zu bevorzugen, die dem Client tatsächlich
; Dateien bereitgestellt haben. Die folgenden Registrierungsoptionen bestimmen, wann ein
; Server in der Liste nach oben verschoben wird. Der Wert ServerHistoryUseCount gibt an, wie oft
; ein Server verwendet werden muss, bevor er an den Anfang der Liste verschoben wird,
; der Wert ServerHistoryCacheTime gibt an, wie lang er (in Sekunden) gespeichert werden soll.
REG52=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryUseCount, 3, , REG_DWORD
REG53=HKEY_LOCAL_MACHINE,
SOFTWARE\LANDesk\ManagementSuite\WinClient\SoftwareDistribution\ServerHistoryCacheTime, 3600, , REG_
DWORD
```

Grundlegendes zur UNC-Authentifizierung

Wenn Sie bevorzugte Server hinzufügen (**Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**), stellen Sie auch Anmeldeinformationen bereit, die die Geräte beim Zugriff auf den bevorzugten Server verwenden sollen. Aus Sicherheitsgründen sollten Sie sicherstellen, dass des bei den Anmeldeinformationen eine Aufteilung zwischen reinem Lesezugriff und Schreibzugriff gibt. (Näheres hierzu unter "Informationen zum Dialogfeld "Eigenschaften des bevorzugten Servers"" auf Seite 920.) Verwaltete Geräte erhalten Anmeldeinformationen für schreibgeschützten Zugriff vom Core und verwenden sie beim Download von Dateien zur Authentifizierung beim bevorzugten Server.

Wenn Sie bevorzugte Server verwenden, die dem Dialogfeld **Serveranmeldeinformationen** hinzugefügt wurden, brauchen Sie Ihre Paketfreigaben nicht mehr als Null-Session-Freigaben zu konfigurieren, wie dies bei früheren Versionen notwendig war. Solange die Anmeldeinformationen, die Sie für den bevorzugten Server bereitgestellt haben, mit der Paketfreigabe funktionieren (klicken Sie auf **Anmeldeinformationen testen** im Dialog **Konfiguration**), sollten verwaltete Geräte auf die Freigabe zugreifen können.

Konfigurieren von Quellen und Spiegelung

Ein Quellserver hostet die Dateien, die auf einen bevorzugten Server repliziert werden müssen, Die Anzahl der Quellserver ist beliebig. Sie müssen Anmeldeinformationen für schreibgeschützten Zugriff für den Quellserver angeben. Auf dem Quellserver deaktivieren Sie die anonyme Authentifizierung, um sicherzustellen, dass die Anmeldeinformationen für den schreibgeschützten Zugriff mit der Standard-Windows-Authentifizierung funktionieren.

Bei der Replikation von Dateien von Quellservern können vorhandene Dateien auf der Zielfreigabe des bevorzugten Servers auf zweierlei Arten behandelt werden.

1. Vorhandene Dateien auf der Freigabe bleiben unberührt und neue bzw. geänderte Dateien werden einfach kopiert.
2. Die Spiegelung wird aktiviert, so dass neue bzw. geänderte Dateien kopiert und vorhandene Dateien, die nicht auf dem Quellserver existieren, aus der Freigabe des bevorzugten Servers gelöscht werden.

Seien Sie vorsichtig, wenn Sie sich entscheiden, die Spiegelung zu aktivieren. Vorhandene Dateien, die nicht auf dem Quellserver für diese Freigabe existieren, werden dabei gelöscht. Stellen Sie sicher, dass Sie alle wichtigen Dateien, die nur auf der Freigabe des bevorzugten Servers vorliegen, vor der Aktivierung der Spiegelungsfunktion verschieben.

Wenn Sie die Spiegelung aktivieren sollten Sie außerdem sicherstellen, dass die gespiegelte Freigabe nur von einer Quelle für die Datenreplikation verwendet wird. Wenn Daten aus mehreren Quellen auf eine gespiegelte Freigabe repliziert werden, führt dies zu Konflikten, da die gespiegelte Replikation alle Daten löscht, die nicht Teil der Spiegelung sind.

So aktivieren Sie die Spiegelung für eine Quelle

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie in der Baumstruktur **Quellen** mit der rechten Maustaste auf die Quelle, die gespiegelt werden soll, und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Seite **Spiegelung** die Option **Spiegelung aktivieren** aus.
4. Klicken Sie auf **Speichern**.

Verwendung eines Quellenrepräsentanten

Ein Quellenrepräsentant ist ein verwaltetes Windows-Gerät, das Dateien auf dem Quellserver indexiert. Quellenrepräsentanten sind ein optionaler Teil der Inhaltsreplikation. Wenn sich auf Ihrem Quellserver Tausende von Dateien befinden, kann es einige Zeit in Anspruch nehmen, bis der Replikator die Dateien selbst indexiert hat, insbesondere wenn dieser Replikator nicht über eine Verbindung mit niedriger Latenz zur Quelle verfügt. In einem solchen Fall lassen sich Replikationen beschleunigen, wenn ein verwaltetes Windows-Gerät in der Nähe vom Quellserver oder am Quellserver selbst als Quellenrepräsentant ausgewiesen wird, da der Replikator den Dateiindex dann sehr schnell vom Quellenrepräsentanten abrufen kann.

Jedes verwaltete Windows-Gerät kann die Funktion des Quellenrepräsentanten übernehmen. Es muss sich dabei nicht um einen dedizierten Computer oder Server handeln. Um seinen Zweck zu erfüllen, sollte das Gerät eine Verbindung mit niedriger Latenz und hoher Geschwindigkeit zum Quellserver herstellen können. Wenn es sich beim Quellserver um ein verwaltetes Windows-Gerät handelt (und nicht um ein SAN- oder Linux-Gerät), dann kann sich der Quellenrepräsentant auf dem Quellserver befinden.

Der Quellenrepräsentant verwendet die von Ihnen definierten Serveranmeldeinformationen zur Erstellung einer XML-Datei mit Informationen zu sämtlichen Dateien auf der Quellfreigabe. Diese Datei wird bei Bedarf erstellt, maximal jedoch einmal pro Stunde. Sie müssen weder manuell eine Laufwerkszuordnung zum Quellserver vornehmen noch irgendwelche Netzwerkverbindungen zum Quellserver herstellen. Dies wird automatisch von den Verwaltungsagenten übernommen.

Wenn ein Replikationstask gestartet wird, der einen Quellenrepräsentanten verwendet, entscheidet der Replikator anhand der vom Quellenrepräsentanten bereitgestellten XML-Datei , welche Dateien repliziert werden müssen. Die Beteiligung des Quellenrepräsentanten am Replikationstask ist in dem Moment abgeschlossen, in dem die XML-Datei an den Replikator übergeben wurde.

Zuweisen eines Quellenrepräsentanten

Ein Quellenrepräsentant ist ein verwaltetes Windows-Gerät, das Dateien auf dem Quellserver indexiert. Quellenrepräsentanten sind ein optionaler Teil der Inhaltsreplikation. Wenn sich auf Ihrem Quellserver Tausende von Dateien befinden, kann es einige Zeit in Anspruch nehmen, bis der Replikator die Dateien selbst indexiert hat, insbesondere wenn dieser Replikator nicht über eine Verbindung mit niedriger Latenz zur Quelle verfügt. In einem solchen Fall lassen sich Replikationen beschleunigen, wenn ein verwaltetes Windows-Gerät in der Nähe vom Quellserver oder am Quellserver selbst als Quellenrepräsentant ausgewiesen wird, da der Replikator den Dateiindex dann sehr schnell vom Quellenrepräsentanten abrufen kann.

Jedes verwaltete Windows-Gerät kann die Funktion des Quellenrepräsentanten übernehmen. Es muss sich dabei nicht um einen dedizierten Computer oder Server handeln. Um seinen Zweck zu erfüllen, sollte das Gerät eine Verbindung mit niedriger Latenz und hoher Geschwindigkeit zum Quellserver herstellen können. Wenn es sich beim Quellserver um ein verwaltetes Windows-Gerät handelt (und nicht um ein SAN- oder Linux-Gerät), dann kann sich der Quellenrepräsentant auf dem Quellserver befinden.

So weisen Sie einen Quellenrepräsentanten zu

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie in der Baumstruktur **Quellen** mit der rechten Maustaste auf die Quelle, für die Sie einen Repräsentanten bestimmen möchten, und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Seite **Quellenrepräsentant** das Gerät aus, das als Quellenrepräsentant fungieren soll und klicken Sie auf die Schaltfläche **Auswählen**. Um sicherzustellen, dass Sie das richtige Gerät ausgewählt haben, können Sie die Geräteattribute unten auf der Seite überprüfen oder auf **Inventar** klicken, um das Inventar des Geräts anzuzeigen.
4. Klicken Sie auf **Speichern**.

Zuweisen eines Replikators

Ein Replikator ist ein verwaltetes Windows-Gerät, das Dateien von einem Quellserver auf einen bevorzugten Server kopiert. Auf diesem Replikator sollte hinreichend Speicherplatz vorhanden sein, damit er die Daten von allen Verteilungsquellen im lokalen Cache für die Softwareverteilung speichern kann. Wenn der Replikator nicht genügend Speicherplatz besitzt, muss er unter Umständen bei jedem Replikationstask einige Dateien von der Quelle herunterladen. Jeder Replikator kann mehrere Quellen auf mehrere bevorzugte Server replizieren.

So weisen Sie einen Replikator zu

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie mit der rechten Maustaste auf die Baumstruktur **Replikatoren** und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Seite **Identifikation** das Gerät aus, das als Replikator fungieren soll und klicken Sie auf die Schaltfläche **Auswählen**. Um sicherzustellen, dass Sie das richtige Gerät ausgewählt haben, können Sie die Geräteattribute unten auf der Seite überprüfen oder auf **Inventar** klicken, um das Inventar des Geräts anzuzeigen.
4. Klicken Sie auf **Speichern**.
5. Klicken Sie in der Baumstruktur **Replikatoren** mit der rechten Maustaste auf den neuen Replikator und klicken Sie dann auf **Einstellungen jetzt anwenden**.

Sie können einen Replikator auch sehr zügig bestimmen, indem Sie ein Gerät vom Baum **Netzwerkansicht** auf den Baum **Replikatoren** des Fensters zur Inhaltsreplikation ziehen.

HINWEIS: Stellen Sie sicher, dass der Freigabename auf der Quelle und auf den bevorzugten Servern identisch ist. Wenn beispielsweise der Freigabename auf Ihrem Quellserver "shareddata" lautet, muss der Zielfreigabename auf dem bevorzugten Server ebenfalls "shareddata" lauten. Replikatoren erstellen zwar alle erforderlichen Ordner unterhalb des Freigabenamens, die Freigabe selbst kann jedoch nicht vom Replikator erstellt werden.

Der Grund hierfür ist, dass nur der Servername im vollständigen Paketpfad ersetzt wird, wenn verwaltete Geräte einen bevorzugten Server für den Download von Paketdateien verwenden. Der Rest des Pfads ab dem Freigabenamen bleibt exakt so, wie er im ursprünglichen Verteilungspaket lautet.

Replikationsplanung

Die Replizierung erfolgt erst, nachdem Sie einen Replizierungstask geplant haben. Replikationstasks unterscheiden sich von Softwareverteilungstasks. Replikationstasks können nur vom Bereich **Inhaltsreplikation** aus geplant werden.

Sie können entweder einen "On-Demand"-Replikationstask oder einen wiederkehrenden Replikationstask planen. Einmalige Replikationstasks eignen sich zum Testen der Replikation und anfänglichen Konfiguration der Server für die Replikation.

Sobald Sie eine funktionierende Replikationskonfiguration haben, sollten Sie zur Automatisierung der Replikation wiederkehrende Replikationstasks verwenden, die Sie über die Eigenschaften des bevorzugten Servers oder die Replikatoreigenschaften konfigurieren. Im Anschluss daran können Sie die Replikationszeitpläne, den Fortschritt und Status der Replikation in der Taskstruktur des Bereichs **Inhaltsreplikation** an den Strukturknoten ablesen.

HINWEIS: Sie können die Replikation entweder vom Startmenü eines bevorzugten Servers oder eines Replikators aus planen.

So starten Sie einen Inhaltsreplikationstask sofort

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie auf die Struktur **Replikatoren**, klicken Sie mit der rechten Maustaste auf den Replikator,

den Sie planen wollen, und klicken Sie dann auf **Inhaltsreplikation jetzt starten**.

3. Daraufhin wird ein Statusdialogfeld angezeigt, in dem Sie den Replikationsstatus überwachen können.

So planen Sie einen Inhaltsreplikationstask

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie auf die Struktur **Replikatoren**, klicken Sie mit der rechten Maustaste auf den Replikator, den Sie planen wollen, und klicken Sie dann auf **Inhaltsreplikation planen**.
3. Im Bereich **Geplante Tasks** wird daraufhin ein neuer geplanter Task angezeigt.
4. Konfigurieren Sie den neuen geplanten Task, indem Sie mit der rechten Maustaste darauf klicken und dann **Eigenschaften** auswählen.
5. Der Task wird zum konfigurierten Zeitpunkt ausgeführt

So planen Sie einen wiederkehrenden Inhaltsreplikationstask

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie auf die Baumstruktur **Replikatoren**, klicken Sie mit der rechten Maustaste auf den Replikator, den Sie planen wollen und klicken Sie dann auf **Replikatoreigenschaften**.
3. Klicken Sie in der Baumstruktur auf **Einstellungen** und dann auf **Planen**.
4. Klicken Sie in der Symbolleiste auf .
5. Konfigurieren Sie den Zeitplan wie gewünscht. Weitere Informationen hierzu finden Sie unter "Informationen zur Seite "Planen" des ausgewählten Replikators" auf Seite 923.
6. Klicken Sie auf **Speichern**, um das Dialogfeld zu schließen.

So löschen Sie einen wiederkehrenden Replikationstask

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie auf den Baum **Replikatoren**, klicken Sie mit der rechten Maustaste auf den Replikator, den Sie planen wollen und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie in der Baumstruktur auf **Einstellungen** und dann auf **Planen**.
4. Wählen Sie den Zeitplan aus, den Sie löschen möchten, und klicken Sie in der Symbolleiste auf .

Aktualisieren von Replikationseinstellungen

Replikatoren prüfen jedes Mal, wenn sie ausgeführt werden, ob neue Einstellungen vorliegen. Wenn Sie die Einstellungen bei einem Replikator ändern, den Zeitplan aber beibehalten, erhält der Replikator die aktualisierten Einstellungen automatisch beim nächsten Ausführen. Wenn Sie jedoch den Zeitplan des Replikators ändern, empfängt der Replikator diese Änderungen erst zu dem ursprünglich für die Ausführung geplanten Zeitpunkt.

Wurde für einen Replikator beispielsweise ursprünglich eine Ausführung pro Monat geplant und Sie ändern das Intervall auf einmal pro Woche, kann es sein, dass es einen ganzen Monat dauert, bis der Zeitplan tatsächlich aktualisiert wird.

Wenn Sie Zeitpläne für die Replikation ändern, sollten Sie im Anschluss daran einen Task "Einstellungen übernehmen" planen, um die Replikatoren mit dem neuen Zeitplan und den neuen Einstellungen zu aktualisieren.

So aktualisieren Sie die Replikationseinstellungen sofort

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie in der Baumstruktur mit der rechten Maustaste auf den bevorzugten Server oder den Replikator, den Sie aktualisieren möchten, und klicken Sie dann auf **Einstellungen jetzt anwenden**.

Überwachung des Replikationsfortschritts

Den Fortschritt, den Status und den Verlauf eines Replikationstasks können Sie in der Strukturansicht des Bereichs **Inhaltsreplikation** einsehen. Die Strukturansicht weist folgende Knoten auf:

- **Alle Tasks:** Eine Übersicht aller laufenden, ausstehenden und nicht geplanten Replikationstasks.
  - **Wird ausgeführt:** Aktive Replikationstasks.
  - **Ausstehende Tasks:** Replikationstasks, deren Ausführung geplant ist.
  - **Nicht geplant:** Replikationstasks, für die keine Ausführung in der Zukunft geplant ist.
- **Taskverlauf:** Bereits ausgeführte Tasks.

Die Taskansichten zeigen lediglich den Status des letzten Tasks. Sie zeigt nicht den gesamten Taskverlauf, da die Replikation in vielen Umgebungen so häufig stattfindet, dass ein vollständiges Protokoll sehr schnell unüberschaubar wäre.

Hilfe zur Dateireplikation

Informationen zum Dialogfeld "Eigenschaften des bevorzugten Servers"

Das Dialogfeld "Eigenschaften des bevorzugten Servers" verwenden Sie, um Ihre bevorzugten Server zu konfigurieren. Weitere Informationen finden Sie unter "Bevorzugte Server und Inhaltsreplikation" auf Seite 912.

So öffnen Sie das Dialogfeld "Eigenschaften des bevorzugten Servers"

1. Klicken Sie auf **Extras > Verteilung > Inhaltsreplikation / Bevorzugte Server**.
2. Klicken Sie in der Baumstruktur **Inhaltsreplikation** mit der rechten Maustaste auf **Bevorzugte Server (Ziele)** und klicken Sie dann auf **Neuer bevorzugter Server**. Sie können auch mit der rechten Maustaste auf einen vorhandenen bevorzugten Server klicken und dann auf **Eigenschaften** klicken.

Informationen zur Seite "Konfiguration"

Geben Sie auf der Seite **Konfiguration** die Serverinformationen und die Anmeldeinformationen für den schreibgeschützten Zugriff ein. Verwaltete Geräte verwenden diese Informationen, um eine Verbindung zum bevorzugten Server herzustellen.

- **Servername:** Der auflösbare Computername des bevorzugten Servers.
- **Beschreibung:** Die Serverbeschreibung. Diese erscheint in der Baumstruktur **Replikatoren** in der Spalte **Details**.
- **Benutzername:** Der Benutzername für schreibgeschützten Serverzugriff.
- **Kennwort:** Das Kennwort für den von Ihnen eingegebenen Benutzernamen.
- **Kennwort bestätigen:** Geben Sie hier das Kennwort für den von Ihnen eingegebenen Benutzernamen nochmals ein.

- **Anmeldeinformationen testen:** Testen Sie die Anmeldeinformationen, um sicherzustellen, dass diese für den Server gültig sind.

Informationen zur Seite "IP-Adressbereiche"

Die Seite **IP-Adressbereiche** verwenden Sie, um eine erste und eine letzte IP-Adresse für einen Adressbereich einzugeben. Nur Geräte mit IP-Adressen innerhalb dieses Bereichs können Downloads von diesem Server versuchen. Sie können mehrere IP-Adressbereiche eingeben.

- **Erste IP-Adresse:** Die erste IP-Adresse des Bereichs.
- **Letzte IP-Adresse:** Die letzte IP-Adresse des Bereichs.
- **Hinzufügen:** Fügt den IP-Adressbereich zur Liste hinzu.
- **Löschen:** Löscht den ausgewählten IP-Adressbereich.

Informationen zur Seite "Ausgewählter Replikator"

Die Seite "Ausgewählter Replikator" verwenden Sie, um das verwaltete Windows-Gerät auszuwählen, das als Replikator eingesetzt werden soll. Ein Replikator hat die Aufgabe, Daten von einem Quellserver auf das bevorzugte Serverziel zu kopieren.

- **Auswählen:** Markieren Sie das Gerät, das Sie als Replikator verwenden möchten, und klicken Sie dann auf **Auswählen**, um es als Replikator zu bestimmen.
- **Inventar:** Sobald Sie den Replikator ausgewählt haben, können Sie auf diese Schaltfläche klicken, um das Inventar des Geräts anzuzeigen und zu verifizieren, dass es sich tatsächlich um das gewünschte Gerät handelt.
- **Löschen:** Hebt die Auswahl des Geräts als Replikator auf.

Informationen zur Seite "Anmeldeinformationen für das Schreiben"

Die Seite "Anmeldeinformationen für das Schreiben" verwenden Sie, um die Anmeldeinformationen für den schreibberechtigten Zugriff auf den bevorzugten Server zu definieren. Der Replikator verwendet diese Informationen, um eine Verbindung zum bevorzugten Server herzustellen, über die ein Replikator neue oder geänderte Dateien auf einen bevorzugten Server replizieren kann.

- **Benutzername:** Der Benutzername, der die Berechtigung zum Schreibzugriff auf den Server besitzt.
- **Kennwort:** Das Kennwort für den von Ihnen eingegebenen Benutzernamen.
- **Kennwort bestätigen:** Geben Sie hier das Kennwort für den von Ihnen eingegebenen Benutzernamen nochmals ein.
- **Anmeldeinformationen testen:** Testen Sie die Anmeldeinformationen, um sicherzustellen, dass diese für den Server gültig sind.

Informationen zur Seite "Quellen"

Die Seite **Quellen** verwenden Sie für die Konfiguration der Quellpfade, die auf bevorzugte Server kopiert werden sollen.

- **Liste "Quellpfade":** Zeigt die von Ihnen konfigurierten Quellen. Wählen Sie eine Quelle aus dieser Liste aus.
- **Einbeziehen:** Fügt die ausgewählte Quelle zur Liste **Einbezogene Quellpfade** hinzu. Sobald eine Quelle in der Liste **Einbezogene Quellpfade** steht, wird ihr Inhalt bei der Ausführung des Replikationstasks auf den bevorzugten Server repliziert, den Sie konfigurieren.
- **Neu:** Öffnet ein neues Dialogfeld für Quelleneigenschaften, in dem Sie eine neue Quelle konfigurieren können, wenn die von Ihnen gewünschte Quelle noch nicht konfiguriert wurde.

- **Ausschließen:** Entfernt die ausgewählte Quelle aus der Liste **Einbezogene Quellpfade**.
- **Einbezogene Quellpfade:** Zeigt Quellen, deren Inhalte auf den bevorzugten Server repliziert werden, den Sie konfigurieren.

Informationen zum Dialogfeld "Replikatoreigenschaften"

Das Dialogfeld **Replikatoreigenschaften** verwenden Sie, um einen Replikator zu konfigurieren.

Informationen zur Seite "Identifikation"

Die Seite "Identifikation" verwenden Sie, um das verwaltete Windows-Gerät auszuwählen, das als Replikator eingesetzt werden soll. Ein Replikator hat die Aufgabe, Daten von einem Quellserver auf das bevorzugte Serverziel zu kopieren.

- **Auswählen:** Markieren Sie das Gerät, das Sie als Replikator verwenden möchten, und klicken Sie dann auf **Auswählen**, um es als Replikator zu bestimmen.
- **Inventar:** Sobald Sie den Replikator ausgewählt haben, können Sie auf diese Schaltfläche klicken, um das Inventar des Geräts anzuzeigen und zu verifizieren, dass es sich tatsächlich um das gewünschte Gerät handelt.
- **Löschen:** Hebt die Auswahl des Geräts als Replikator auf.

Informationen zur Seite "Bevorzugte Server (Ziele)"

- Liste **Bevorzugter Server**: Zeigt alle bevorzugten Server, die Sie konfiguriert haben. Verschieben Sie Server aus dieser Liste in die Liste **Einbezogene Server**.
- **Einbeziehen:** Verschiebt die ausgewählten bevorzugten Server aus der Liste **Bevorzugte Server** in die Liste **Einbezogene Server**.
- **Ausschließen:** Verschiebt die ausgewählten bevorzugten Server aus der Liste **Einbezogene Server** in die Liste **Bevorzugte Server**.
- Liste **Einbezogene Server**: Die bevorzugten Server in dieser Liste bilden die Ziele für den Replikator, den Sie konfigurieren.

Informationen zu den Seiten "Einstellungen" des ausgewählten Replikators

Die Seiten "Einstellungen" des ausgewählten Replikators verwenden Sie, um die Ausführungsoptionen und den Zeitplan für den Replikator zu konfigurieren.

Informationen zur Seite "Einstellungen"

Auf der Seite "Einstellungen" können Sie die Versionsnummer der Replikatoreinstellungen und die zuletzt vom Replikator gemeldete, aktuelle Revisionsnummer einsehen.

- **Revision der aktuellen Einstellungen:** Zeigt die aktuelle Revisionsnummer. Bei jeder Änderung und Speicherung der Replikatoreinstellungen erhöht sich der Wert für die Revision der aktuellen Einstellungen um eins.
- **Letzte vom Replikator angewendete Revision:** Bei jedem Ausführen prüft der Replikator, ob aktualisierte Einstellungen vorliegen und meldet dann die von ihm verwendete Revisionsnummer der Einstellungen.
- **Letzter Bericht:** Zeigt das Datum und die Uhrzeit an, zu der der Replikator das letzte Mal ausgeführt wurde.

Informationen zur Seite "Ausführungsoptionen" des ausgewählten Replikators

Die Seite "Ausführungsoptionen" des ausgewählten Replikators verwenden Sie zum Konfigurieren der Ausführungsoptionen, wie zum Beispiel der Bandbreitenoptionen und der Einstellungen für die Benutzeroberfläche.

- **WAN-Brandbreiteneinstellungen** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. WAN-Verbindungen sind in der Regel langsamer, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen niedrigeren Prozentsatz einzustellen.
- **LAN-Brandbreiteneinstellungen** Passt die Priorität dieses spezifischen Tasks gegenüber anderem Netzwerkverkehr an. Je höher der mit dem Schieberegler eingestellte Wert, desto größer die Bandbreite, die von diesem Task im Verhältnis zu allem anderen Verkehr im Netzwerk verwendet wird. LAN-Verbindungen sind in der Regel schneller als WAN-Verbindungen, daher empfiehlt es sich in den meisten Fällen, diesen Schieberegler auf einen höheren Prozentsatz einzustellen, als den Prozentsatz für WAN.
- **Fortschrittsdialog anzeigen:** Zeigt ein Dialogfeld mit einer Fortschrittsanzeige auf dem Replikator an. Bei deaktivierter Option, wird der Task im Hintergrund ohne Benachrichtigung oder Statusanzeigen ausgeführt.
- **Peerdownload zulassen:** Bei aktivierter Option prüft der Replikator zunächst lokale Peers auf Quelldateien, die repliziert werden sollen. Wenn der Replikator die Datei nicht auf einem Peer finden kann, holt er die Datei vom Quellserver. Die Option kann dazu beitragen, den Datenverkehr auf Ihrem Quellserver zu reduzieren.
- **Dateispeicherung im Cache für maximal:** Replizierte Dateien verbleiben im lokalen Verteilungscache auf dem Replikator. Indem die Dateien im Cache bleiben, muss der Replikator die Dateien nicht bei jedem Replikationstask vom Quellserver übertragen. Wenn Sie aus irgendeinem Grund den Replikator dazu zwingen möchten, die im Cache zwischengespeicherten Dateien in regelmäßigen Abständen zu aktualisieren, aktivieren Sie diese Option und geben Sie die Anzahl der Tage ein.

  Im Allgemeinen kann diese Option deaktiviert bleiben, da alle Dateien, die sich in der Quelle ändern automatisch im lokalen Cache aktualisiert werden, wenn der Replikationstask das nächste Mal ausgeführt wird.
- **WAN-Brandbreiteneinstellungen** Aktivieren Sie diese Option, wenn Sie bei der Push-Übertragung von Dateien auf die Ziele Ihre WAN-Brandbreiteneinstellungen verwenden möchten.
- **LAN-Brandbreiteneinstellungen** Aktivieren Sie diese Option, wenn Sie bei der Push-Übertragung von Dateien auf die Ziele Ihre LAN-Brandbreiteneinstellungen verwenden möchten.

Informationen zur Seite "Planen" des ausgewählten Replikators

Die Seite **Planen** des ausgewählten Replikators verwenden Sie, um den Zeitplan für die Ausführung des Replikators zu definieren. Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird das Dialogfeld "Inhaltsreplikation planen" angezeigt. Von Ihnen konfigurierte Zeitpläne erscheinen im Listenfeld "Planen". Sie können einen vorhandenen Zeitplan ändern oder löschen, indem Sie diesen auswählen und auf die entsprechende Schaltfläche klicken.

Informationen zum Dialogfeld "Inhaltsreplikation planen"

- Zeit:
  - **Start:** Klicken Sie auf diese Option, um einen Kalender anzuzeigen, in dem Sie den Tag angeben, an dem der Task starten soll. Wenn Sie einen Tag auswählen, können Sie auch die Tageszeit eingeben. Die Standardwerte für diese Optionen sind das aktuelle Datum und die aktuelle Uhrzeit.
  - **Wiederholen nach:** Wenn Sie möchten, dass sich der Task wiederholt, klicken Sie auf das Listenfeld und wählen **Minuten**, **Stunden** oder **Tage**. Geben Sie dann im ersten Feld an, wie lang das ausgewählte Intervall dauern soll (z. B. 10 Tage).
  - **Wöchentlich zwischen:** Wenn Sie möchten, dass der Task zwischen bestimmten Wochentagen ausgeführt wird, wählen Sie den ersten und letzten Tag aus.
  - **Monatlich zwischen:** Wenn Sie möchten, dass der Task zwischen bestimmten Tagen des Monats ausgeführt wird, wählen Sie das Anfangs- und Enddatum aus.
- Maximale Dauer:
  - **Bis zum Abschluss der Replikation ausführen:** Bei Aktivierung dieser Option wird der Replikationstask bis zum Abschluss ausgeführt.
  - **Beenden nach:** Bei Aktivierung dieser Option wird die Replikation nach der von Ihnen angegebene Zeitspanne gestoppt. Bei der nächsten geplanten Replikation wird der Task an der Stelle fortgesetzt, an der er gestoppt wurde. Diese Option erweist sich dann als nützlich, wenn Sie die Replikation nachts über eine langsame Verbindung ausführen und vermeiden wollen, dass der durch die Replikation verursachte Datenverkehr den Netzwerkverkehr tagsüber während der regulären Arbeitszeit beeinträchtigt.
- Bevorzugte Server zur Aktualisierung auswählen:
  - **Alle verknüpften bevorzugten Server aktualisieren:** Die Replikation erfolgt für alle mit diesem Replikator verknüpften bevorzugten Server.
  - **Nur die folgenden bevorzugten Server aktualisieren:** Die Replikation erfolgt ausschließlich für die von Ihnen ausgewählten bevorzugten Server. Diese Option sollten Sie verwenden, wenn Sie die Replikation für unterschiedliche bevorzugte Server zu unterschiedlichen Zeiten planen möchten.

Informationen zum Dialogfeld "Inhaltsreplikationstask planen"

Das Dialogfeld **Inhaltsreplikationstask planen** verwenden Sie, um die einmalige Ausführung eines Replikationstasks zu definieren. Nachdem Sie mithilfe diese Dialogfelds einen geplanten Task erstellt haben, müssen Sie im Extra **Geplante Tasks** eine Zeit für die Ausführung des Tasks definieren

- **Taskname:** Der Name für diesen Task, der im Extra "Geplante Tasks" angezeigt wird.
- **Geplanten Task erstellen:** Erstellt einen geplanten Task.
- **Richtlinie erstellen:** Erstellt eine Richtlinie.
- **Ausgewählte oder (implizierte) Replikatoren zur Zielliste hinzufügen:** Wenn Sie einen Replikator oder bevorzugten Server ausgewählt haben, ist diese Option verfügbar. Diese Option fügt dann den ausgewählten Replikator und zusätzliche Replikatoren als Taskziele hinzu, auf die in den Konfigurationen von verknüpften bevorzugten Servern verwiesen wird.
- **Nur die ausgewählten bevorzugten Server replizieren:** Wenn Sie einen Replikator ausgewählt haben, ist diese Option verfügbar. Diese Option erstellt einen Task, der nur auf die von Ihnen ausgewählten Replikatoren abzielt.

Informationen zum Task "Einstellungen anwenden" planen

Den Task '"Einstellungen anwenden" planen' verwenden Sie, um den Replikator mit neuen Einstellungen zu aktualisieren. Der Zugriff auf dieses Dialogfeld erfolgt über die Symbolleiste des Bereichs **Inhaltsreplikation**. Replikatoren prüfen vor der Ausführung automatisch, ob aktualisierte Einstellungen vorliegen. Ein Task vom Typ "Einstellungen anwenden" erweist sich als nützlich, wenn Sie einen Computer als neuen Replikator zugewiesen haben. Wenn Sie diesen Task planen, wird die Replikatorsoftware auf dem Computer installiert.

- **Taskname:** Der Name für diesen Task, der im Extra "Geplante Tasks" angezeigt wird.
- **Geplanten Task erstellen:** Erstellt einen geplanten Task.
- **Richtlinie erstellen:** Erstellt eine Richtlinie.
- **Keine Replikatoren zu diesem Task hinzufügen:** Lässt die Zielliste leer, so dass Sie Ihre eigenen Replikatorziele im Extra "Geplante Tasks" hinzufügen können.
- **Alle veralteten Replikatoren hinzufügen:** Fügt alle Replikatoren hinzu, die eine Einstellungsversion gemeldet haben, die nicht der neuesten Version entspricht.
- **Nur (neue) Replikatoren hinzufügen, die noch nicht berichtet haben:** Fügt neu bestimmte Replikatoren hinzu, die zuvor weder ausgeführt wurden noch berichtet haben. Damit werden neue Replikatoren mit den neuesten Einstellungen konfiguriert.

Mandantenverwaltung

Mandantenverwaltung – Übersicht

Die Mandantenverwaltung ist ein Add-On zu LANDesk Management Suite, das Sie separat erwerben können. Die Mandantenverwaltung gibt Ihnen die Möglichkeit, verwaltete Geräte und Konfigurationen nach Unternehmen zu unterteilen. Wenn Sie für die Verwaltung von mehreren Unternehmen oder eigenständigen Organisationen innerhalb Ihres eigenen Unternehmens zuständig sind, mussten Sie in der Vergangenheit unter Umständen für jeden Standort einen separaten LANDesk Management Suite-Coreserver bereitstellen. Anschließend hätten Sie sich dann bei jedem einzelnen Core anmelden müssen, um das jeweilige Unternehmen bzw. die jeweilige Organisation zu verwalten.

Wird die Mandantenverwaltung Seite and Seite mit einer LANDesk Cloud Services Appliance eingesetzt, so reduziert dies den Bedarf an mehreren Coreserver erheblich. Sobald Sie die Mandantenverwaltung konfigurieren, werden die für die Mandanten konfigurierten Geräte in separaten Bereichen innerhalb der Konsole angezeigt. So können Sie bei der Verwendung der Konsole sicherstellen, dass Sie stets die Assets des richtigen Mandanten verwalten.

Jeder von Ihnen erstellte Mandant erhält sein eigenes Team und seinen eigenen Bereich für die Benutzerverwaltung. Sie können den spezifischen Mandantenteams und -bereichen Konsolenbenutzer zuweisen, die dann für deren Verwaltung zuständig sind.

Für jedem Mandanten können außerdem Kontaktinformationen und Vertragsbedingungen verknüpft sowie die Nutzung von LANDesk Lizenzen verfolgt werden.

Die wesentlichen Schritte zur Konfiguration der Mandantenverwaltung sind folgende:

1. Erstellen Sie im Mandantenverwaltungstool einen Mandanten.
2. Fügen Sie im Benutzerverwaltungstool Konsolenbenutzer zu einem Team oder einem Bereich hinzu, für das bzw. den der Mandant sichtbar ist.
3. Erstellen Sie im Agentenkonfigurationstool eine Agentenkonfiguration, wählen Sie den passenden Mandanten im Mandantenbereich aus und stellen Sie diese dann bereit.
4. Verwenden Sie die Mandantengruppen in der Konsole, um die Mandanten zu verwalten.

Erstellung eines Mandanten

Zur Erstellung eines Mandanten verwenden Sie das Mandantenverwaltungstool (**Tools > Verwaltung > Mandantenverwaltung >** Schaltfläche **Neue Mandantendefinition**). Sie müssen jedem Mandanten einen eindeutigen Mandantennamen und eine eindeutige Kennung geben. Der Mandantenname darf nicht mit einem der vorhandenen RBA-Bereichs- oder Teamnamen übereinstimmen. Die Mandantenkennung kann nur bei der erstmaligen Erstellung des Mandanten bearbeitet werden.

Als Mandantenkennung wird standardmäßig eine GUID verwendet, die Sie jedoch in eine beliebige Kombination von Buchstaben (A –Z, a – z), Ziffern und Strichen ändern können. GUIDs sind unter Umständen schwer im Gedächtnis zu behalten, daher sollten Sie erwägen, stattdessen die Kundennummer oder ähnliches zu verwenden.

Die übrigen Informationen im Dialogfeld **Mandantenkonfiguration** sind optional. Wenn Sie Kontaktinformationen, Vertragsbedingungen oder Lizenzinformationen hinzufügen, werden viele dieser Informationen innerhalb des Mandantenverwaltungstools in Spalten angezeigt.

Die Lizenzinformationen dienen nur der Information. Die Anzahl der Mandanten wird von der Mandantenverwaltung nicht auf die Anzahl der von Ihnen eingegebenen **Zugewiesenen LANDesk Lizenzen** beschränkt. Die Verfolgung zugewiesener Lizenzen kann sich unter anderem bei der Abrechnung als nützlich erweisen.

Verwenden Sie die Registerkarte Notizen, um ggf. Zusatzinformationen hinzuzufügen.

Bei der Erstellung eines Mandanten wird automatisch ein entsprechendes Team und ein entsprechender Bereich für die Benutzerverwaltung mit dem selben Namen für diesen Mandanten erstellt. Sie müssen Konsolenbenutzer, die für die Verwaltung dieses Mandanten zuständig sein sollen, zum Benutzerverwaltungsteam und -bereich hinzufügen. Nur Konsolenbenutzer, die Mitglieder des Benutzerverwaltungsteams des Mandanten sind, können die Gruppen des Mandanten in den verschiedenen Konsolenbereichen einsehen.

Wenn Sie einen Mandanten umbenennen, wird der Name des mit diesem verknüpften Benutzerverwaltungsteams und Benutzerverwaltungsbereichs automatisch auch geändert sowie jedes weitere Vorkommen des Namens an anderen Stellen in der Konsole.

Erstellen eines Mandanten

Einen Mandanten erstellen Sie, wenn Sie verwaltete Geräte nach Organisation oder Unternehmen unterteilen möchten.

So erstellen Sie einen Mandanten

1. Klicken Sie auf **Extras > Administration > Mandantenverwaltung**.
2. Geben Sie einen eindeutigen **Mandantennamen** ein.
3. Ändern Sie die **Eindeutige Kennung**, wenn Sie die Zufalls-GUID nicht verwenden möchten. Gültige Zeichen sind: A – Z, a – z, 0 – 9 und Bindestriche.
4. Falls gewünscht können Sie zusätzliche, für den Mandanten relevante Daten hinzufügen.
5. Klicken Sie auf **Speichern**.

So fügen Sie Konsolenbenutzer hinzu, die den Mandanten verwalten

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Doppelklicken Sie auf das neue Team, das nach dem Namen Ihres Mandanten benannt wurde.
3. Wählen Sie die Konsolenbenutzer aus, die bei diesem Mandanten die Geräteverwaltung übernehmen werden.
4. Klicken Sie auf **OK**.

So fügen Sie Konsolenbenutzer zum Bereich des Mandanten hinzu

1. Klicken Sie auf **Extras > Administration > Benutzerverwaltung**.
2. Klicken Sie mit der rechten Maustaste auf den neuen Bereich, der entsprechend Ihrem Mandantennamen benannt ist und klicken Sie dann auf **Eigenschaften**.
3. Wählen Sie auf der Seite **Benutzer und Gruppen** die Konsolenbenutzer aus, die bei diesem Mandanten die Geräteverwaltung übernehmen werden.
4. Klicken Sie auf **OK**.

Hinzufügen von Mandantengeräten

Nachdem Sie einen Mandanten erstellt haben, können Sie Geräte zum Mandanten hinzufügen, indem Sie eine aktualisierte Agentenkonfiguration bereitstellen, die eine Zuweisung des Mandanten zu den verwalteten Geräten dieses Mandanten vornimmt.

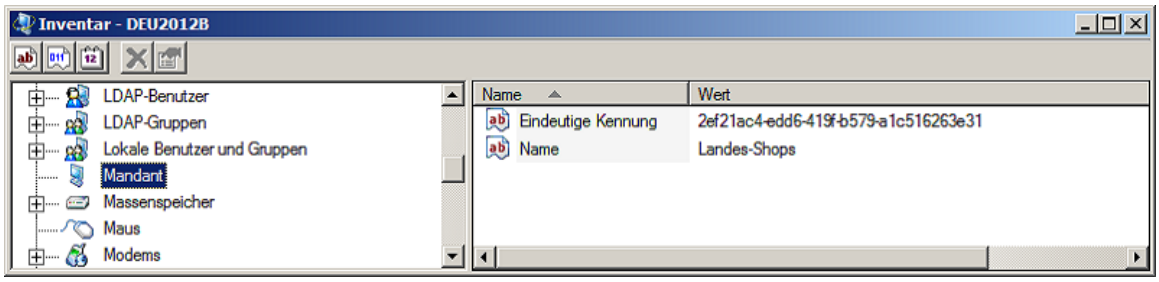
Jeder von Ihnen erstellte Mandant hat seine einige Teamgruppe im Dialogfeld der Agentenkonfiguration. Diese Teamgruppe verwenden Sie, um Agentenkonfigurationen zu organisieren, die für den jeweiligen Mandanten eindeutig sind.

Das Dialogfeld „Agentenkonfiguration“ enthält eine Seite **Mandant**, auf der Sie den mit der Agentenkonfiguration verknüpften Mandanten auswählen können.

Wenn Sie einen Mandanten einer Agentenkonfiguration zuweisen, die sich nicht in der Teamgruppe des Mandanten befindet, wird diese Konfiguration nicht automatisch in die Teamgruppe des Mandanten verschoben. Sie müssen sie vielmehr bei Bedarf manuell dorthin verschieben oder kopieren.

Haben Sie bereits eine Agentenkonfiguration an Mandantengeräte verteilt, müssen Sie nicht noch einmal eine vollständige Agentenkonfiguration bereitstellen, wenn Sie die Mandanteneinstellung auf einem Gerät aktualisieren möchten. Nachdem Sie einen Mandanten in der von Ihnen gewünschten Agentenkonfiguration zugewiesen haben, verwenden Sie vielmehr die Symbolleistenschaltfläche **Agenteneinstellungs-Update planen**, um die Einstellungen auf den Zielgeräten zu aktualisieren.

Der Inventarscanner schließt die gefundene Mandantenkennung in die Inventarscans ein. Der Mandantenname und die eindeutige Kennung wird in der Strukturansicht "Inventar" des Geräts unterhalb des Knotens **Mandant** angezeigt.



Mandantengeräte hinzufügen

Sie fügen Geräte zu einem Mandanten hinzu, indem Sie einer Agentenkonfiguration einen Mandanten zuweisen und dann diese Agentenkonfiguration an die Geräte verteilen, die diesem Mandanten gehören.

So fügen Sie Mandantengeräte hinzu

1. Klicken Sie auf **Extras > Konfiguration > Agentenkonfiguration**.
2. Klicken Sie im Baum **Agentenkonfiguration** auf die Agentenkonfigurationsgruppe, die mit Ihrem Mandantennamen übereinstimmt. Wenn Sie eine vorhandene Agentenkonfiguration verwenden möchten, kopieren Sie sie und fügen Sie sie in die Gruppe des Mandanten ein.
3. Vergewissern Sie sich, dass im Dialogfeld **Agentenkonfiguration** das Kontrollkästchen **Dieser Konfiguration einen Mandanten zuweisen** aktiviert ist und Sie den Mandanten ausgewählt haben, der für diese Agentenkonfiguration festgelegt werden soll.
4. Klicken Sie auf **Speichern**.

5. Wenn Sie eine vorhandene Agentenkonfiguration auf Mandantengeräten aktualisieren, klicken Sie auf die Symbolleistenschaltfläche **Agenteneinstellungs-Update planen**. Andernfalls stellen Sie die vollständige Agentenkonfiguration bereit.
6. Fügen Sie die Geräte, die dem Mandanten gehören, zu einem geplanten Task hinzu und planen Sie dessen Ausführung.

Löschen von Mandanten und Mandantengeräten

Wenn Sie einen Mandanten löschen, wird die Gruppe des Mandanten aus den Konsolentools entfernt, die darauf verweisen. Wenn Sie einen Mandanten löschen, werden Sie gefragt, ob Sie das mit ihm verknüpfte Objekteigentum, wie z. B. Agentenkonfigurationen, einem anderen Konsolenbenutzer neu zuweisen möchten. Wenn Sie dies nicht tun, wird das Eigentum des verwaisten Objekts auf den Root-Konsolenadministrator zurückgesetzt.

Die eindeutige Kennung des Mandanten verbleibt auf den Mandantengeräten und wird beim Entfernen des Mandanten nicht entfernt. Wenn Sie wollen, können Sie die eindeutige Kennung von Mandantengeräten entfernen, indem Sie erneut Agentenkonfigurationseinstellungen bereitstellen, die keinen Mandanten umfassen. Verbleibt die eindeutige Kennung auf Mandantengeräten, hat dies zur Folge, dass der Inventarscanner die Inventardaten für die eindeutige Kennung auffüllt. Da aber mit dem Gerät kein Mandantenname mehr verknüpft ist, gehört das Gerät dann nicht zur Teamgruppe des Mandanten.

Löschen eines Mandanten oder Mandantengeräts

So löschen Sie einen Mandanten

1. Klicken Sie auf **Extras > Administration > Mandantenverwaltung**.
2. Wählen Sie den Mandanten aus, den Sie löschen möchten, und drücken Sie die Taste **Entf** auf der Tastatur.
3. Wenn die Mandantenobjekte nicht an den Root-Administrator zurückfallen sollen, und Sie diese erneut einem Konsolenbenutzer oder einem Team zuordnen wollen, wählen Sie den gewünschten Benutzer bzw. das gewünschte Team aus.
4. Klicken Sie auf **OK**.

So entfernen Sie ein Gerät von einem Mandanten

1. Wählen Sie im Agentenkonfigurationstool eine Agentenkonfiguration aus, bei der kein Mandant ausgewählt ist.
2. Klicken Sie auf die Symbolleistenschaltfläche **Agenteneinstellungs-Update planen**.
3. Fügen Sie die Geräte, die Sie von dem Mandanten entfernen möchten, zum geplanten Task hinzu und planen Sie dessen Ausführung.

Verwalten von Geräten bei einem Mandanten

Sobald Sie die folgenden Schritte ausgeführt haben, wird der Mandant in vielen Bereichen der Konsole als Element angezeigt.

1. Erstellen eines Mandanten
2. Zuweisen von Konsolenrechten zur Verwaltung des Mandanten
3. Hinzufügen von Geräten zum Mandanten

Der Mandant wird unter anderem in folgenden Bereichen angezeigt:

- in der Netzwerkansicht unter **Geräte**, **Virtuelle Betriebssystemhosts**, **Abfragen** und **Bereiche,**
- in der Toolbox "Administration" unter **Spaltensatzkonfiguration** und **Benutzerverwaltung**,
- in der Toolbox "Verteilung" unter **Verteilungsmethoden**, **Verteilungspakete** und **Skripte verwalten**,
- im Extra "Energieverwaltung" und
- in der Toolbox "Sicherheit und Compliance" unter **Patch und Compliance** und **Sicherheitskonfigurationen**.

Sie können dann in diesen Tools die Teamgruppe des Mandanten verwenden, um die Geräte anzuzeigen und zu verwalten, die einem Mandanten gehören. Nur Konsolenbenutzer, die über die entsprechenden Rechte zum Verwalten eines Mandanten verfügen, können den betreffenden Mandanten in der Konsole sehen.

Ein einfacher Weg, Mandantengeräte in einem geplanten Task anzusprechen, besteht darin, den Bereich des Mandanten aus der **Netzwerkansicht** zu ziehen und auf dem gewünschten Task abzulegen.

HINWEIS: Bei Windows-Geräten wird die eindeutige Kennung des Mandanten zur Registrierung hinzugefügt:

HKLM\SOFTWARE\LANDesk\ManagementSuite\WincClient\Tenant\TenantUID

Bei Macintosh-Geräten wird die eindeutige Kennung des Mandanten zur einer plist hinzugefügt:

/Library/Preferences/com.landesk.ldms.plist

Anwendungsvirtualisierung

LANDesk Application Virtualization

LANDesk Application Virtualization ist ein von LANDesk Software, Inc. separat angebotenes Add-On zu LANDesk Management Suite. LANDesk Application Virtualization virtualisiert Anwendungen mithilfe der Thinstall-Technologie, wobei die virtualisierten Dateien zusammen mit der Anwendung und mit den .DLL/Gerätetreiberabhängigkeiten in eine einfache, eigenständige EXE-Datei gepackt werden.

Die virtualisierten Anwendungen werden in einer isolierten Umgebung ausgeführt, ohne die Windows-Installation zu ändern, unter der sie ausgeführt werden. Virtualisierte Anwendungen laufen sogar auf Geräten mit gesperrter Konfiguration ("Locked-Down"-PCs), ohne zusätzliche Privilegien vorauszusetzen.

Weitere Informationen finden Sie in der Dokumentation zu LANDesk Application Virtualization. Wenn Sie LANDesk Application Virtualization mit Management Suite verwenden, können Sie virtualisierte Anwendungen bereitstellen und verwalten.

HINWEIS: Verwendung von Nicht-LANDesk-Versionen von Thinstall
Die LANDesk Application Virtualization-Version von Thinstall verfügt über Management Suite-spezifische Anpassungen. Andere Version von mit Thinstall virtualisierten Anwendungen arbeiten möglicherweise nicht wie erwartet mit der Softwarelizenzüberwachung oder mit dem Inventarscanner zusammen.

Verteilen einer virtualisierten Anwendung

Virtualisierte Anwendungen bestehen im Allgemeinen aus einer oder aus mehreren EXE-Dateien. Sie können die ausführbaren Dateien dieser virtualisierten Anwendung mithilfe der Softwareverteilung auf verwalteten Geräten bereitstellen. Die virtualisierten Anwendungspakete unterstützen jede Art von Softwareverteilungsmethode, einschließlich der "Ausführung von Quelle". Wenn Sie ein virtualisiertes Anwendungspaket mit der Option "Ausführung von Quelle" bereitstellen, verwenden die verwalteten Geräte eine Programmverknüpfung, um die EXE-Datei der virtualisierten Anwendung über das Netzwerk auszuführen.

So erstellen Sie ein virtualisierten Anwendungspaket

1. Verwenden Sie LANDesk Application Virtualization, um die EXE-Datei Ihrer virtualisierten Anwendung zu erstellen.
2. Klicken Sie auf **Extras > Verteilung > Verteilungspakete**.
3. Klicken Sie mit der rechten Maustaste auf die gewünschte Paketgruppe, und klicken Sie dann auf **Neues Verteilungspaket > Neues virtualisiertes Anwendungspaket**.
4. Geben Sie im Dialogfeld **Verteilungspakete** die Paketinformationen ein und ändern Sie nach Bedarf die Optionen. Beachten Sie, dass Sie den Paketnamen, eine Beschreibung und Primärdatei eingeben müssen. Weitere Informationen zu den einzelnen Seiten finden Sie in der **Hilfe**.
5. Die Seite **Shortcut** ist die einzige für virtualisierte Anwendungen spezifische Seite. Geben Sie den **Namen** für das Shortcutsymbol ein. Sie können auch festlegen, ob Sie das Symbol auf dem **Desktop** und/oder im **Startmenü** anzeigen möchten. Wenn Sie "Startmenü" auswählen, können Sie zudem den **Namen des Programmordners** eingeben, in dem der Shortcut gespeichert wird. Der Ordnerpfad, den Sie eingeben, wird unter **Alle Programme** angezeigt.

6. Klicken Sie auf **OK**, wenn Sie den Vorgang abgeschlossen haben. Ihr Skript wird unter dem Strukturelement für den von Ihnen ausgewählten Pakettyp und Eigentümer angezeigt.

Wenn Sie eine virtualisierte Anwendung bereitstellen, kopiert die Softwareverteilung die ausführbaren Dateien in folgenden Ordner auf verwalteten Geräten:

- %programfiles%\LANDesk\VirtualApplications\<Verteilungsquellpfad>

Der vollständige Pfad der virtualisierten Anwendung enthält den Quellpfad der Softwareverteilung, um Probleme mit doppelt vorhandenen Dateinamen zu vermeiden. Wenn der Quellpfad Ihrer Verteilung vapps\myapp.exe lautet, lautet der Pfad auf verwalteten Geräten %programfiles%\LANDesk\VirtualApplications\vapps\myapp.exe.

Sie können den Standardpfad der virtualisierten Anwendung bei Bedarf auf der Seite **Softwareverteilung** des Dialogfelds **Agentenkonfiguration** ändern.

Einige virtualisierte Anwendungen erfordern mehrere EXE-Dateien. Wenn dies der Fall ist, können Sie ein separates Verteilungspaket für diese zusätzlichen virtualisierten EXE-Dateien erstellen. Wenn Sie dann ein Verteilungspaket für die Haupt-EXE-Datei der virtualisierten Anwendung erstellen, können Sie alle zusätzlichen abhängigen EXE-Pakete als Abhängigkeiten einschließen. Auf diese Weise werden die abhängigen EXE-Dateien automatisch installiert, falls sie noch nicht vorhanden sind.

Abhängige EXE-Dateien müssen sich bei der Erstellung der Verteilungspakete im selben freigegebenen Ordner befinden. So wird gewährleistet, dass die abhängigen Pakete an denselben Ordner auf dem verwalteten Gerät verteilt werden. Wenn die abhängigen EXE-Dateien sich nicht im selben Ordner auf dem verwalteten Gerät befinden, lassen sie sich nicht ausführen.

Das erste Mal, wenn eine virtualisierte Anwendung auf einem Gerät ausgeführt wird, wird das Dialogfeld "Thinstall runtime license agreement" angezeigt. Benutzer müssen auf **Fortsetzen** klicken, um die virtualisierte Anwendung auszuführen. Dieser Schritt muss in der Regel nur ein Mal ausgeführt werden.

Sandbox der virtualisierten Anwendung

Standardmäßig erstellen virtualisierte Anwendungen temporäre Dateien, die sie für ihre Ausführung benötigen, in folgendem Ordner:

- Dokumente und Einstellungen\<Benutzername>\Anwendungsdaten\Thinstall\

Der Inventarscanner scannt diesen Ordner nicht, um falsche Berichte bzgl. der auf dem System vorhandenen Anwendungen zu verhindern.

Verwenden der Inventar- und Softwarelizenzüberwachung mit virtualisierten Anwendungen

EXE-Dateien virtualisierter Anwendungen, die mit LANDesk Application Virtualization erstellt wurden, verfügen über zusätzliche Eigenschaftsinformationen, die Management Suite bei der Inventarisierung und Softwarelizenzüberwachung unterstützen. Wenn Sie in Windows Explorer mit der rechten Maustaste auf die EXE-Datei einer virtualisierten Anwendung und dann auf **Eigenschaften** klicken, werden diese zusätzlichen Versionsinformationen angezeigt:

- **ThinstallLicense:** LANDesk Application Virtualization-Lizenztyp und E-Mail-Adresse für die Registrierung.

- **ThinstallVersion:** LANDesk Application Virtualization-Packager-Version, mit der das Paket erstellt wurde.

Sie können diese Informationen in Ihren Inventarabfragen zur Suche nach virtualisierten Anwendungen verwenden, die vom Inventarscanner gescannt wurden. Im Allgemeinen spiegeln die Eigenschaften von EXE-Dateien virtualisierter Anwendungen diejenigen der EXE-Hauptdatei innerhalb der virtualisierten Anwendung wieder. In der Inventaransicht des Geräts werden virtualisierte Anwendungen in der Liste **Software > Paket** angezeigt. Virtualisierte Anwendungen in dieser Liste verfügen über ein Attribut vom Typ "Virtuelle Anwendung" mit dem Wert "Ja".

Einige Anwendungen stellen jedoch keine Versionsinformationen bereit, bevor sie virtualisiert werden. In diesem Fall erscheinen sie nicht als virtualisierte Anwendungen im Inventar, obwohl sie virtualisiert sind.

EXE-Dateien virtualisierter Anwendungen werden nur dann automatisch vom Inventarscanner gescannt, wenn Sie mit MODE=ALL scannen. Wenn Sie MODE=ALL nicht verwenden und Inventarinformationen zu virtualisierten Anwendungen in die Datenbank einfügen möchten, müssen Sie die Informationen zur EXE-Datei der virtualisierten Anwendung in der Softwarelizenzüberwachung unter **Inventar > Dateien > Liste "Zu scannen"** hinzufügen. Der Inventarscanner sieht nur die EXE-Datei der virtualisierten Anwendung. Er führt keinen Scan innerhalb der EXE-Datei durch.

Die Softwarelizenzüberwachung erkennt automatisch virtualisierte Anwendungen und schließt sie in die Liste **Produktdefinitionen > Automatisch erkannt** ein. Die automatische Anwendungserkennung der Softwarelizenzüberwachung verwendet nicht den Inventarscanner. Die Softwarelizenzüberwachung verwendet stattdessen die Erkennung über das Startmenü oder die Desktop-Verknüpfung mit der Anwendung.

Eine erkannte virtualisierte Anwendung in der Liste **Automatisch erkannt** führt in ihrer Dateiliste nur die einzelne EXE-Datei der virtualisierten Anwendung, doch basiert die Produktdefinition nach wie vor auf dem Produkt innerhalb der EXE-Datei der virtualisierten Anwendung. Die Softwarelizenzüberwachung schaut nicht in die EXE-Datei der virtualisierten Anwendung und kann deshalb keine anderen Dateien einschließen, die normalerweise einem Produkt zugewiesen werden, wenn es ohne Virtualisierung installiert wird.

Webkonsole

Informationen zur Webkonsole

Mit der Management Suite Webkonsole können Sie Systemverwaltungstasks automatisieren und Desktops, Server sowie mobile Geräte steuern. Die Webkonsole unterscheidet sich dahingehend von der LANDesk Management Console, dass der Zugriff über einen Browser erfolgt und nicht über eine unter Windows ausführbare Datei.

Die Webkonsole nutzt die Infrastruktur des bestehenden Netzwerks, um Verbindungen mit den von ihr verwalteten Geräten herzustellen. Damit wird die Verwaltung Ihrer Netzwerke deutlich vereinfacht, ganz gleich, ob Sie ein kleines Netzwerk oder eine große Unternehmensumgebung verwalten, und selbst dann, wenn Sie gerade nicht an Ihrem Platz sind.

Die Webkonsole kann auf jedem Windows-Computer ausgeführt werden, auf dem folgende Browser und Plugins installiert sind:

- Internet Explorer 8 oder höher
- Mozilla Firefox 4.0 oder höher
- Google Chrome
- Adobe Flash Player 9 oder höher

Starten der Webkonsole

So starten Sie die Webkonsole

1. Öffnen Sie einen Webbrowser auf einem Netzwerkcomputer.
2. Geben Sie in das Adressfeld oben im Browser eine URL ein, die auf dem Coreserver zeigt, gefolgt von **/remote** (im Format http://<NameDesWebservers>/remote).
3. Wird ein Anmeldefenster angezeigt, geben Sie Ihren Windows-Benutzernamen und Ihr Kennwort für den Coreserver ein, mit dem Sie eine Verbindung herstellen möchten, und klicken Sie auf **OK**.
4. Nach der Authentifizierung werden im linken Navigationsfenster Verknüpfungen für die Tasks angezeigt, zu deren Ausführung Sie berechtigt sind, z. B. Erstellen von Abfragen, Remotesteuerung von Clients, Verteilen von Software und Anzeigen von Berichten.

Klicken Sie hier, um eine Beschreibung des Dialogfelds **Anmelden** anzuzeigen.

Verwenden Sie dieses Dialogfeld, um die Konsole zu starten und eine Verbindung mit einem Coreserver herzustellen.

- **Benutzername:** Identifiziert einen Benutzer. Es kann sich dabei um einen Benutzer mit Administratorrechten oder um einen anderen Benutzertyp mit eingeschränktem Zugriff handeln. Dieser Benutzer muss ein Mitglied der LANDesk Management Suite-Gruppe auf dem Coreserver sein. Wenn Sie eine Verbindung mit einem Remote-Coreserver herstellen, geben Sie den Domänennamen und Benutzernamen ein.
- **Kennwort:** Das Kennwort des Benutzers.

Fehlerbehebung

- Wenn die Geräteliste und Schaltflächen beim Starten der Konsole nicht angezeigt werden, müssen Sie den Coreserver aktivieren.

- Wenn Sie die URL zu den Webkonsolenseiten nicht kennen, wenden Sie sich an die Person, die die Webkonsole installiert hat; in der Regel ist dies der Netzwerkadministrator Ihres Standorts.
- Wenn nicht alle Links im linken Navigationsfenster angezeigt werden, verwendet Ihr Netzwerkadministrator wahrscheinlich die rollenbasierte Administration oder die Option "Sicherheit auf Funktionsebene" in Management Suite, wodurch Sie an der Ausführung bestimmter Tasks gehindert werden, für die Sie eigentlich Rechte besitzen.

Verwenden der Webkonsole

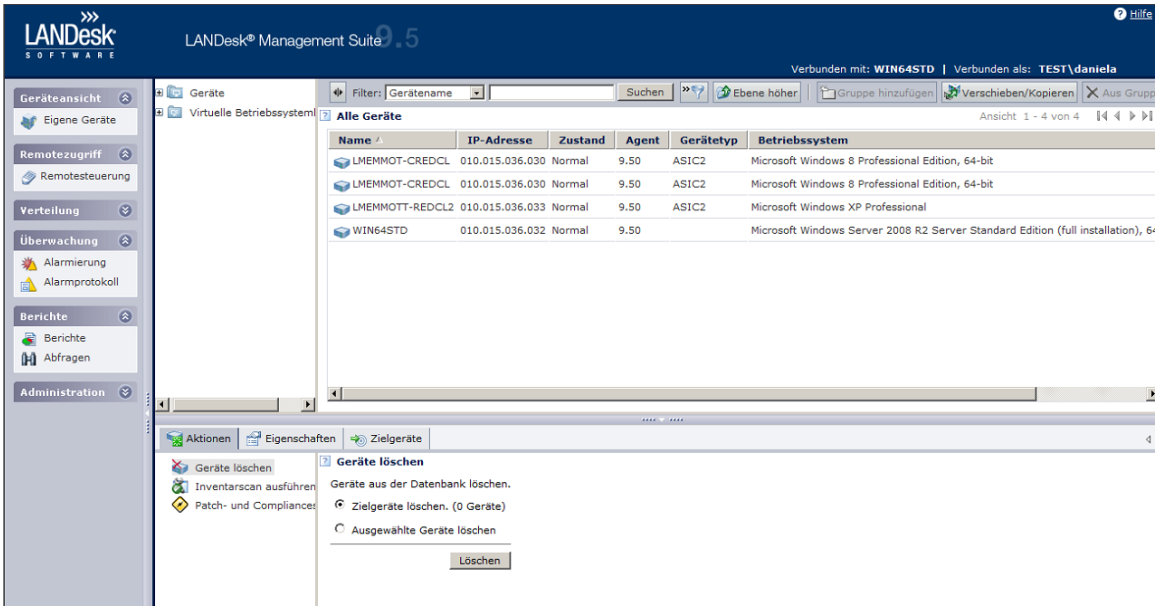
Dieses Thema beschreibt die Management Suite Webkonsole und wie sie verwendet wird.

Denken Sie bitte daran, dass Sie, wenn Sie ein Extra nicht sehen können, vermutlich nicht die erforderlichen Rechte zum Anzeigen des Extras haben. Diese Rechte werden über die Zugriffsrechte und den Gerätebereich bestimmt, der Ihnen vom Management Suite Administrator zugewiesen wurde.

Layout der Webkonsole

Die Webkonsole weist vier wesentliche Bereiche auf, mit denen Sie arbeiten:

- die Titelleiste
- die Toolbox
- den Extrabereich
- den Aktionsbereich



Die **Titelleiste** zeigt das Gerät an, bei dem Sie angemeldet sind, und den Benutzer, unter dessen Namen Sie sich angemeldet haben. Sie enthält einen Link zur Hilfe, über den Hilfethemen für die Webkonsole aufgerufen werden.

Die Toolbox zeigt die verfügbaren Extras bzw. Tools, die gruppiert unter Überschriften angezeigt werden. Zum Erweitern oder Schließen einer Gruppe klicken Sie auf die Chevrons neben einer Überschrift.

Der Inhalt des rechten Bereichs der Konsole wechselt je nachdem, welches Extra gerade verwendet wird. Wenn dieser Bereich unterteilt ist, wird der obere Bereich als **Extrabereich** oder Fensterbereich "Extra" und der untere Bereich als **Aktionsbereich** oder Fensterbereich "Aktion" bezeichnet. Der Extrabereich zeigt die wesentlichen Elemente des von Ihnen ausgewählten Extras. Im Aktionsbereich wählen Sie in der Regel Aktionen aus oder sehen die Ergebnisse des Tasks ein, an dem Sie gerade arbeiten.

Sie können die Größe der Fensterausschnitte und Spalten der Webkonsole ändern. Auch die Größe der Toolbar-Elemente kann reduziert oder erweitert werden, damit sie besser zu erkennen sind.

HINWEIS: Damit Dialogfelder und Fenster ordnungsgemäß angezeigt werden, muss die Website von Management Suite zur Liste der zulässigen Websites im Popupblocker des Browsers hinzugefügt werden.

Dieses Thema bietet Ihnen weiterhin die folgenden Informationen:

- Die Liste "Eigene Geräte"
- Gerätesymbole
- Verwenden von Kontextmenüs
- Verwenden von Extras
- Anzeigen von Geräteeigenschaften

Die Liste "Eigene Geräte"

Die Liste **Eigene Geräte** ist das Hauptfenster, das beim Starten der Webkonsole angezeigt wird und bildet den Ausgangspunkt für die meisten Extras. Sie umfasst die folgenden Gruppen und Untergruppen. Zusätzlich zu diesen Gruppen können Sie – abhängig von Ihren Zugriffsrechten und Gerätebereichen – eigene Gruppen erstellen, die die Geräteverwaltung zusätzlich vereinfachen.

Einige der häufig verwendeten Funktionen in dieser Liste sind folgende:

- Klicken Sie mit der rechten Maustaste auf ein Gerät in der Liste **Geräte**, um verfügbare Optionen für das Gerät anzuzeigen, beispielsweise "Ping", "Remotesteuerung" und "Ziel".
- Um mehrere aufeinander folgende Einträge in einer Liste auszuwählen, klicken Sie auf den ersten Eintrag, drücken und halten die **Umschalttaste** gedrückt und klicken dann auf den letzten Eintrag.
- Um mehrere nicht aufeinander folgende Einträge in einer Liste auszuwählen, drücken und halten Sie die **Strg**-Taste gedrückt und klicken dann auf jeden einzelnen auszuwählenden Eintrag.
- Wenn Sie in der Liste **Alle Geräte** auf ein Gerät klicken, wird ein vollständiges Geräteinventarfenster mit allen Inventarinformationen zu dem Gerät angezeigt.

Alle Geräte

Die Liste **Alle Geräte** führt - basierend auf dem Bereich des Benutzers - in einer einfachen Aufstellung (keine Untergruppen) die Geräte des zurzeit angemeldeten Benutzers auf. Wenn eine Verbindung zu einem bestimmten Coreserver besteht, kann der Administrator jedes Gerät sehen, das von diesem Coreserver verwaltet wird. Produktbenutzer sind hingegen eingeschränkt und sehen nur die Geräte, die zu dem ihnen zugewiesenen Bereich gehören (ein Bereich basiert auf einer Datenbankabfrage oder einem Verzeichnisstandort).

Geräte, die Produktagenten ausführen (Standard Management Agent und Inventaragent), werden automatisch in der Liste **Alle Geräte** angezeigt, nachdem sie vom Inventarscanner in die Coredatenbank eingelesen werden. In der Regel wird dieser Scan zum ersten Mal während der ersten Gerätekonfiguration durchgeführt. Sobald ein Gerät in die Coredatenbank gescannt wurde, gilt es als verwaltetes Gerät – d. h., dass es von nun an von diesem Coreserver verwaltet werden kann.

Da die Gruppe **Alle Geräte** automatisch mithilfe eines Inventarscans gefüllt wird, müssen Sie möglicherweise nie manuell nach Geräten suchen. Um jedoch Geräte zu finden, die nicht bereits in der Coredatenbank enthalten sind (oder um nicht verwaltete Geräte in die Gruppe "Verwaltete Geräte" zu verschieben), können Sie mit dem Geräteerkennungstool das Netzwerk nach Geräten durchsuchen.

Die Gruppe **Alle Geräte** stellt für jedes Gerät die nachstehend beschriebenen Informationen zur Verfügung. Um eine Spalte zu sortieren, klicken Sie auf ihre Überschrift. Wenn Sie erneut auf die Überschrift klicken, wird die Sortierung rückgängig gemacht. Doppelklicken Sie auf **Alle Geräte**, um die Liste zu öffnen.

- **Name:** Der Hostname des Geräts, z. B. der Windows-Computername.
- **IP-Adresse:** Die IP-Adresse des Geräts.
- **Zustand:** Der System- und Verfügbarkeitsstatus des Geräts. Unterstützte Zustände sind u. a. "Normal", "Warnung" oder "Kritisch".
- **Agent:** Der aktuell auf dem Gerät ausgeführte Agent.
- **Gerätetyp:** Zeigt die auf dem Computer installierte Hardware an (Intel AMT, IPMI, ASIC oder IPMI Advanced).
- **Betriebssystem:** Das vom Gerät ausgeführte Betriebssystem.
- **Aktiv seit:** Gibt an, seit welchem Datum und welcher Uhrzeit das Gerät unterbrechungsfrei gearbeitet hat (in der Zeitzone der Datenbank).
- **LaunchPad:**

Wenn auf einem Gerät keine Agenten installiert sind, enthalten nur die Spalten "Name" und "IP-Adresse" Informationen. In einigen Fällen wird auch das Betriebssystem angezeigt.

Wenn Sie ein Gerät auswählen, werden die Eigenschaften des Geräts im Fensterausschnitt **Eigenschaften** unterhalb der Geräteliste angezeigt. Im Bereich **Eigenschaften** werden die wesentlichen Geräteattribute aufgelistet:

- **Kennung:** Die Kennnummer des Geräts. Diese Nummer wird von der Reihenfolge bestimmt, in der das Gerät zur Liste **Alle Geräte** hinzugefügt wurde.
- **IP-Adresse:** Die IP-Adresse des Geräts.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Das Gerätemodell.
- **Prozessorgeschwindigkeit:** Die Geschwindigkeit der Geräte-CPU.
- **Prozessortyp:** Der CPU-Typ des Geräts.

Weitere Aktionen, die im Bereich **Eigenschaften** verfügbar sind, werden unter "Informationen zur Registerkarte "Eigenschaften"" auf Seite 940 beschrieben.

Eigene Geräte

In der Liste **Eigene Geräte** werden die Gerätegruppen angezeigt, die vom gegenwärtig angemeldeten Benutzer erstellt wurden. Gruppen des Typs "Eigene Geräte" sind für andere Benutzer nicht sichtbar und können somit von anderen Benutzern auch nicht verwendet werden.

Öffentliche Geräte:

In der Liste **Öffentliche Geräte** werden Gerätegruppen angezeigt, die von einem Benutzer erstellt wurden, der über Administratorrechte verfügt. Diese Gruppen sind für andere Benutzer sichtbar.

Betriebssystem der virtuellen Hosts

Die Liste **Betriebssystem der virtuellen Hosts** zeigt VMware ESX-Server, die als virtuelle Hosts konfiguriert wurden, die durch die Auswahl der Option "Virtuelle Hosts" in der Geräteerkennungskonfiguration erkannt wurden. Wenn Sie in der Strukturdiagramm auf **Betriebssystem der virtuellen Hosts** oder eine beliebige Untergruppe klicken, werden die Hosts als Endgeräte im Gerätefenster angezeigt. Wenn Sie auf einen Hostnamen in der Strukturansicht klicken, wird der Host als Container und die virtuellen Geräte darauf in der Geräteliste dargestellt.

Gerätesymbole

Gerätesymbole in der Liste **Alle Geräte** zeigen den gegenwärtigen Zustand bzw. Integritätsstatus jedes Geräts an, sofern auf dem Gerät ein Agent vorhanden ist, bei dem die Option **Echtzeitinventar und Überwachung** ausgewählt wurde. Sie können die Zustandsinformationen für jedes Gerät einzeln aktualisieren, indem Sie das Gerät in der Liste **Eigene Geräte** auswählen und dann auf die Schaltfläche **Aktualisieren** klicken.

Es gibt vier verschiedene Statussymbole:

Symbol	Beschreibung
	Gerät mit Normalstatus
	Gerät mit Alarmstatus
	Gerät mit kritischem Status
	Gerät mit unbekanntem Status

HINWEIS: Damit diese Symbole korrekt angezeigt werden, ist eine Farbtiefeneinstellung von mindestens 16 Bit erforderlich. Wenn die Symbole in der Konsole unscharf dargestellt werden, ändern Sie die Farbeinstellungen in den Anzeigeeigenschaften von Windows.

Kontextmenüs

Für alle Elemente in der Konsole, einschließlich Gruppen, Geräte, Abfragen, geplante Tasks, Skripte usw., stehen Kontextmenüs (Kurzbefehlmenüs) zur Verfügung. Kontextmenüs ermöglichen den schnellen Zugriff auf die allgemeinen Tasks und wichtigen Informationen eines Elements.

Sie können das Kontextmenü eines Elements anzeigen, indem Sie mit der rechten Maustaste auf das Element klicken. Wenn Sie beispielsweise in der Liste **Eigene Geräte** mit der rechten Maustaste auf ein verwaltetes Gerät klicken, werden im Kontextmenü in der Regel folgende Optionen eingeblendet:

- **Aus Gruppe entfernen:** Entfernt das Element aus einer benutzerdefinierten Gruppe.
- **Ziel:** Verschiebt das ausgewählte Gerät in die Liste der Zielgeräte. (Wenn in der Zielliste keine Zielgeräte angezeigt werden, klicken Sie auf der Registerkarte **Zielgeräte** auf **Aktualisieren**.)
- **Einen Pingtest mit dem Gerät durchführen:** Stellt sicher, dass das Gerät antwortet.
- **Einen Traceroutetest mit dem Gerät durchführen:** Sendet einen Trace-Route-Befehl, um ein gesendetes und empfangenes Netzwerkpaket sowie die Anzahl von Hops anzuzeigen, die das Paket benötigt, um an sein Ziel zu gelangen.
- **Gerät scannen:** Scannt das Gerät auf Anfälligkeiten. Klicken Sie auf **Scan starten**.
- **DSView starten**: Startet das Add-on "Avocent DSView", sofern es installiert ist.
- **Remotesteuerung:** Startet das Remotesteuerungsfenster, das direkten Zugriff auf das ausgewählte Gerät von der Konsole aus ermöglicht.

Eine komplette Aufstellung der Kontextmenüs von allen Elementen der Konsole würde den Rahmen dieser Hilfe sprengen. Sie können sich jedoch über jedes einzelne Element informieren, indem Sie mit der rechten Maustaste auf das betreffende Element klicken und die verfügbaren Optionen anzeigen.

Verwenden von Extras

Extras sind in der Toolbox in verschieden Abschnitten zusammengruppiert und tragen Überschriften wie **Geräteansicht** und **Remotezugriff**. Zum Erweitern oder Schließen einer Gruppe klicken Sie auf die Chevrons neben einer Überschrift.

Der Administrator sieht alle Extras in der Toolbox. Andere Benutzer sehen nur die Extras (Funktionen), auf die sie aufgrund der ihnen zugewiesenen Rechte Zugriff haben. Wenn ein Benutzer z. B. nicht über das Berichtsrecht verfügt, wird das Extra **Berichte** nicht in der Toolbox angezeigt.

Vollständige Liste der Extras:

- Eigene Geräte:
- **Remotesteuerung:** Steuern Sie Geräte aus der Ferne und tauschen Sie Dateien mit ihnen aus.
- **Avocent DSView:** Zeigen Sie eine Liste mit Geräten an, auf denen Avocent DSView installiert ist. Sie können auf ein Gerät in der Liste doppelklicken, um eine DSView-Sitzung zu starten.
- **Verteilung:** Verteilen Sie Softwarepakete, verwenden Sie benutzerdefinierte Skripte, planen Sie Verteilungen und erstellen Sie Softwareverteilungstasks.
- **LaunchPad Link-Manager:** Mit LANDesk LaunchPad können Sie Links zu Softwarepaketen für Benutzer bereitstellen.
- **Skripts:** Erstellen und verwalten Sie Skripte.
- **Verzeichnis-Manager:** Suchen, öffnen und verwalten Sie Geräte in anderen Verzeichnissen via LDAP (Lightweight Directory Access Protocol).
- **Geplante Tasks:** Zeigen Sie alle Tasks an, die derzeit geplant oder abgeschlossen sind.
- Alarmierung:
- Alarmprotokoll:
- **Berichte:** Verwalten Sie vordefinierte Berichte.
- **Abfragen:** Erstellen und ändern Sie an die Datenbank gerichtete Abfragen, um Geräte zu isolieren, die Ihre Kriterien erfüllen.
- **Voreinstellungen:** Erstellen Sie benutzerdefinierte Inventarattribute und zeigen Sie Lizenzinformationen an.

Anzeigen von Geräteeigenschaften und Inventar

In der Ansicht **Eigene Geräte** können Sie im Handumdrehen Informationen zu einem Gerät anzeigen, indem Sie auf das Gerät in der Liste klicken und im Aktionsbereich **Eigenschaften** auswählen.

Genauere Informationen über das Gerät finden Sie in den Inventardaten des Geräts. Sie können Inventardaten in der Ansicht **Alle Geräte** anzeigen, indem Sie auf das Gerät doppelklicken oder indem Sie die Registerkarte **Inventar anzeigen** im Bereich **Eigenschaften** auswählen, um das Fenster **Inventar** vollständig zu öffnen.

Informationen zur Registerkarte "Eigenschaften"

Auf der Registerkarte "Eigenschaften" können Sie nützliche Informationen zu dem von Ihnen ausgewählten Gerät einsehen. Der Bildschirm enthält eine Kurzübersicht der Eigenschaften und der folgenden Schaltflächen:

- **Inventar anzeigen:** Klicken Sie auf diese Schaltfläche, um das vollständige Inventar des ausgewählten Geräts in einer Strukturansicht zu öffnen. Diese Daten werden vom Inventarscanner erfasst, der sie in der Datenbank speichert. Die Detailansicht zeigt sämtliche für ein Gerät möglicherweise verfügbaren Inventarelemente an, d. h. einige Elemente (die bei dem von Ihnen ausgewählten Gerät nicht aktiviert sind) weisen daher keine Daten auf. Klicken Sie auf ein Element in der Ansicht, um entsprechende Einzelheiten für dieses Gerät anzuzeigen. Um zur Standardansicht zurückzukehren, klicken Sie auf den Gerätenamen in der obersten Ebene der Ansicht.
- **Remotesteuerung:** Startet das Remotesteuerungsfenster, das direkten Zugriff auf das ausgewählte Gerät von der Konsole aus ermöglicht.
- **SSH:** Bietet sicheren Zugriff auf das ausgewählte Linux-Gerät. Wenn das ausgewählte Gerät kein Linux-Gerät ist, ist die Option abgeblendet.
- **SFTP:** Bietet sicheren FTP-Zugriff auf das ausgewählte Linux-Gerät. Wenn das ausgewählte Gerät kein Linux-Gerät ist, ist die Option abgeblendet.

Zielgeräte definieren [Webkonsole]

Mithilfe der Liste **Zielgeräte** können Sie Tasks auf ausgewählten Geräten ausführen, beispielsweise Agenten auf einer ausgewählten Gruppe von Geräten bereitstellen oder einen Scan auf Softwareupdates durchführen.

Es wird empfohlen, maximal 250 Geräte in die Liste aufzunehmen. Die Geräte bleiben in der Liste, bis Ihre Konsolensitzung endet oder abläuft (nach 20 Minuten Inaktivität).

Sie können Geräte als Ziele definieren, indem Sie sie aus einer beliebigen Liste von Geräten auswählen. Wenn die gewünschten Geräte nicht angezeigt werden, verwenden Sie die Symbolleistenschaltfläche **Suchen**. Suchen Sie entweder nach einem bestimmten Gerät oder nach mehreren Geräten gleichzeitig (mithilfe des Platzhalterzeichens % oder *).

Wenn mindestens ein Gerät in der Liste **Zielgeräte** enthalten ist, können Sie einen Task wie das Bereitstellen einer Agentenkonfiguration auf jedem der Zielgeräte durchführen.

So definieren Sie Zielgeräte mit der Webkonsole

1. Klicken Sie in der Liste **Eigene Geräte** oder der Liste **Alle Geräte** auf das Gerät, das Sie als Ziel für eine Aktion auswählen möchten. Mit Umschalt+Mausklick oder Strg+Mausklick können Sie mehrere Geräte auswählen.

2. Klicken Sie auf die Schaltfläche **Ziel**. Wird diese nicht angezeigt, klicken Sie in der Symbolleiste auf die Schaltfläche **Filter** , um die Filteroptionen auszublenden (die Schaltfläche **Ziel** befindet sich ganz rechts).

Die ausgewählten Geräte werden im Aktionsbereich unter der Registerkarte **Zielgeräte** aufgelistet. Sobald die Geräte unter dieser Registerkarte aufgelistet werden, können Sie ein Extra öffnen (beispielsweise die Verteilung) und einen Task zeitlich planen, der auf die Zielgeräte angewendet werden kann.

HINWEIS: Gerätelisten können mehrere Seiten umfassen. Sie müssen daher beim Auswählen der Geräte für die einzelnen Seiten auf die Schaltfläche **Ziel** klicken. Es ist nicht möglich, auf mehreren Seiten Geräte auszuwählen und dann nur ein Mal für alle Seiten auf die Schaltflächen zu klicken.

HINWEIS: Sie können auf den nach unten zeigenden Pfeil unterhalb der Symbolleiste auf der äußersten rechten Seite klicken, um festzulegen, wie viele Geräte Sie pro Seite anzeigen möchten. Sie können bis zu 500 Geräte pro Seite anzeigen. Um die Anzahl der in Gerätelisten angezeigten Geräte permanent zu ändern, klicken Sie auf **Administration > Voreinstellungen > Seiteneinstellungen**.

Filtern der Anzeigeliste [Webkonsole]

Die Liste **Geräte** verfügt über eine Filteroption, mit der Sie festlegen können, welche Geräte in der Liste angezeigt werden. Sie können einen von vier verschiedenen Kriterientypen für die Filterung wählen (Gerätename, IP-Adresse, Betriebssystem oder Anmeldename). Verwenden Sie ein Platzhalterzeichen (% oder *), um einen Bereich von Elementen mit ähnlichen Bezeichnern auszuwählen.

So filtern Sie die Anzeigeliste

1. Klicken Sie auf **Eigene Geräte** und navigieren Sie zu einer Gruppe unter **Geräte**.
2. Sollten die Filteroptionen nicht angezeigt werden, klicken Sie auf die Schaltfläche **Filter** in der Symbolleiste.
3. Wählen Sie in der Liste **Filter** entweder **Gerätename**, **IP-Adresse**, **Betriebssystem** oder **Anmeldename** aus.
4. Legen Sie die Parameter für den Filter fest, indem Sie die entsprechenden Daten in das Textfeld eingeben.

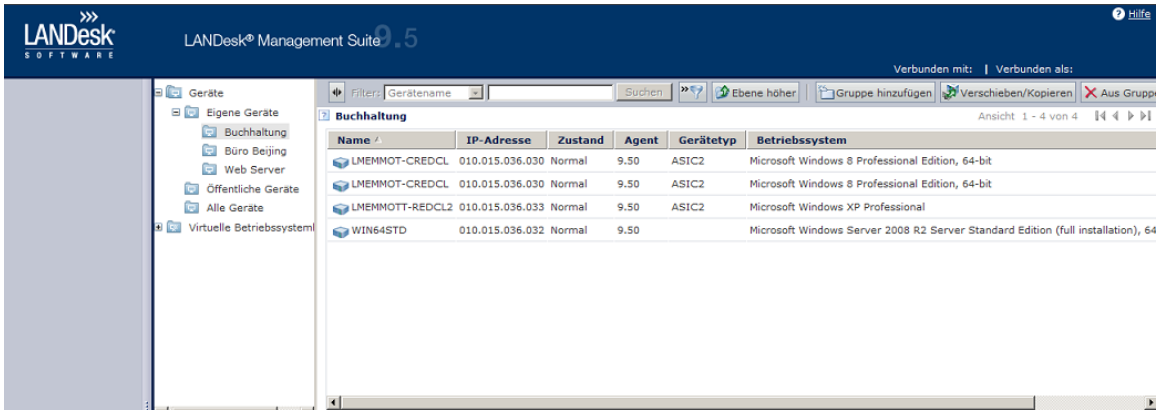
   Folgende Zeichen des erweiterten Zeichensatzes werden in diesem Feld nicht unterstützt: < , > , " , ' , !.

   Wenn Sie beispielsweise nach Gerätename filtern, geben Sie den Hostnamen oder den Computernamen-Bereich ein. Bei der Suche nach Computernamen können Sie Platzhalter verwenden (z. B. *srv).
5. Klicken Sie auf **Suchen**.

Verwenden von Gruppen [Webkonsole]

Zur Vereinfachung des Verwaltungsaufwands können Sie Geräte in Gruppen zusammenfassen. Sie können Gruppen erstellen, um Geräte nach Funktion, Standort, Abteilung, Geräteattribut oder einer anderen Kategorie zu ordnen, die Ihren Anforderungen entspricht. Sie können z. B. eine Webserver-Gruppe für alle als Webserver konfigurierten Server erstellen oder alle Geräte, die ein bestimmtes Betriebssystem ausführen, zu einer Gruppe zusammenfassen.

Die folgende Bildschirmabbildung zeigen drei Gerätegruppen, die vom aktuellen Benutzer erstellt wurden.



Klicken Sie mit der rechten Maustaste auf eine Gruppe, um sie zu öffnen, zu löschen oder alle darin enthaltenen Geräte als Ziel für Aktionen wie eine Softwareverteilung oder eine Agentenbereitstellung auszuwählen.

Die Hauptansicht des Fensters **Geräte** enthält die folgenden Gruppen:

- **Eigene Geräte:** Führt die Gruppen/Geräte für die aktuell angemeldeten Benutzer auf, basierend auf dem Benutzerbereich. Benutzer können nur unter **Eigene Geräte** Untergruppen für Geräte erstellen. Sie können Geräte zur Gruppe **Eigene Geräte** oder zu einer Untergruppe hinzufügen, indem Sie die Geräte aus den Gruppen **Öffentliche Geräte** und **Alle Geräte** kopieren. Alle Benutzer können Gruppen unter **Eigene Geräte** in der Windows-Konsole erstellen.
- **Öffentliche Geräte:** Führt Gruppen bzw. Geräte auf, die ein Administrator aus der Gruppe **Alle Geräte** hinzugefügt hat. Ein Administrator (ein Benutzer, dem das Recht "Administrator" zugewiesen wurde) kann alle Geräte in dieser Gruppe anzeigen, während andere Benutzer nur die Geräte sehen können, die zu ihrem Bereich gehören. Nur Administratoren können Gruppen unter **Öffentliche Geräte** erstellen.
- **Alle Geräte:** Erstellt eine einfache Liste (keine Untergruppen) mit allen Geräten, die für den zurzeit angemeldeten Benutzer (abhängig von dessen Bereich) sichtbar sind. Für einen Administrator führt **Alle Geräte** alle Geräte auf, die in die Coredatenbank gescannt oder dorthin verschoben wurden. Mit dem Standard Management Agent konfigurierte Geräte werden automatisch in der Gruppe/dem Ordner **Alle Geräte** angezeigt, wenn sie mit dem Inventarscanner in die Coredatenbank gescannt werden. Benutzer, einschließlich Administratoren, können keine Gruppen unter **Alle Geräte** erstellen.

Erstellen einer Gerätegruppe [Webkonsole]

Mithilfe von Gruppen können Sie Geräte, die sich in der Liste **Geräte** der Konsole befinden, übersichtlich ordnen. Sie können Gruppen erstellen, um Geräte nach Funktion, Standort, Abteilung, Attribut oder einer anderen Kategorie zu ordnen, die Ihren Anforderungen entspricht. Sie können z. B. eine Marketinggruppe für alle Geräte in der Marketingabteilung erstellen oder alle Geräte mit einem bestimmten Betriebssystem zu einer Gruppe zusammenfassen. Sie können Gruppen in Gruppen platzieren, beispielsweise alle Geräte, die ein bestimmtes Betriebssystem an einem bestimmten Standort ausführen.

Gruppen sind wie folgt gegliedert:

- **Geräte**: Um unter **Geräte** Gruppen erstellen zu können, müssen Sie zuerst **Eigene Geräte** oder **Öffentliche Geräte** auswählen.
- **Eigene Geräte:** Eigene Geräte können nur von dem Benutzer angezeigt werden, der sie erstellt hat.
- **Öffentliche Geräte:** Nur Administratoren können unter **Öffentliche Geräte** Gruppen erstellen oder ändern, jedoch kann jeder Benutzer die Gruppen anzeigen.
- **Alle Geräte:** Es gibt keine Untergruppen unter **Alle Geräte**.

So erstellen Sie eine Gruppe

1. Klicken Sie in der Liste **Geräte** auf **Eigene Geräte** oder **Öffentliche Geräte**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Gruppe hinzufügen**.
3. Geben Sie einen Namen für die neue Gruppe ein und klicken Sie auf **OK**.

So löschen Sie eine Gruppe

1. Klicken Sie in der Geräteansicht der Konsole auf das übergeordnete Element der Gruppe, die Sie löschen möchten.
2. Klicken Sie im Extrabereich mit der rechten Maustaste auf die Gruppe, die Sie löschen möchten, und klicken Sie dann auf **Gruppe löschen**.

Verwenden der Registerkarte "Aktionen" [Webkonsole]

Die Registerkarte **Aktionen** verwenden Sie zum Ausführen folgender Vorgänge auf ausgewählten Servern und Zielgeräten.

- Löschen von Geräten aus der Datenbank
- Ausführen von Inventarscans auf ausgewählten Geräten
- Ausführen von Patch- und Compliancescans auf ausgewählten Geräten

So löschen Sie Geräte aus der Datenbank

Sie können entweder Geräte aus der aktuellen Geräteliste auswählen oder eine Liste von Geräten als Ziel verwenden (was sich insbesondere dann als nützlich erweist, wenn die Geräteliste mehrere Seiten umfasst).

1. Klicken Sie in der Webkonsole auf **Eigene Geräte** und wählen Sie die Geräte bzw. Ziele aus, die gelöscht werden sollen.
2. Klicken Sie auf der Registerkarte **Aktionen** auf **Geräte löschen**. Wählen Sie je nach Bedarf **Zielgeräte löschen** oder **Ausgewählte Geräte löschen**.
3. Klicken Sie auf **Löschen** und bestätigen Sie, dass Sie die Geräte löschen möchten.

Die Löschfunktion kann einzelne oder mehrere Geräte aus einer beliebigen Standardgruppe oder einer benutzerdefinierten Gruppe löschen. Nachdem Sie ein Gerät aus einer Gruppe gelöscht haben, wird es aus allen Listen mit verwalteten/inventarisierten Geräten, einschließlich der Standardgruppe **Alle Geräte**, entfernt.

So führen Sie einen Inventarscan auf ausgewählten Geräten aus

Sie können entweder Geräte aus der aktuellen Geräteliste auswählen oder eine Liste von Geräten als Ziel verwenden (was sich insbesondere dann als nützlich erweist, wenn die Geräteliste mehrere Seiten umfasst).

1. Klicken Sie in der Webkonsole auf **Eigene Geräte** und wählen Sie die Geräte bzw. Ziele aus, die gelöscht werden sollen.
2. Klicken Sie auf der Registerkarte **Aktionen** auf **Inventarscan ausführen**. Wählen Sie je nach Bedarf **Zielgeräte scannen** oder **Ausgewählte Geräte scannen**.
3. Wählen Sie die Art des Scans aus (Nur Hardware, Hardware und Software oder Vollständige Synchronisierung).
4. Klicken Sie auf **Scan**.

Statushinweise zum Fortschritt des Scanvorgangs werden im Aktionsbereich angezeigt.

So führen Sie Patch- und Compliancescans auf ausgewählten Geräten aus

Sie können entweder Geräte aus der aktuellen Geräteliste auswählen oder eine Liste von Geräten als Ziel verwenden (was sich insbesondere dann als nützlich erweist, wenn die Geräteliste mehrere Seiten umfasst).

1. Klicken Sie in der Webkonsole auf **Eigene Geräte** und wählen Sie die Geräte bzw. Ziele aus, die gelöscht werden sollen.
2. Klicken Sie auf der Registerkarte **Aktionen** auf **Patch- und Compliancescan ausführen**. Wählen Sie je nach Bedarf **Zielgeräte scannen** oder **Ausgewählte Geräte scannen**.
3. Wählen Sie die Art des Scans (Sicherheits- und Patchscan, Compliancescan) aus.
4. Klicken Sie auf **Scan**.

Ändern der Seiteneinstellungen [Webkonsole]

Verwenden Sie die Seite **Seiteneinstellungen** zum Festlegen der Darstellungsweise von Seiten, auf denen Geräte aufgelistet oder Grafiken angezeigt werden. Das Health-Dashboard, das über separate Dialoge für die Einstellung von Anzeigenvorgaben verfügt, ist hierin nicht enthalten.

So ändern Sie die Seiteneinstellungen der Webkonsole

1. Klicken Sie in der Toolbox der Webkonsole auf **Administration > Einstellungen**.
2. Klicken Sie auf die Registerkarte **Seiteneinstellungen**.
3. Wählen Sie in der Liste **Diagrammtyp** den Diagrammtyp aus, den Sie unter **Berichte** anzeigen möchten.
4. Geben Sie in das Feld **Elemente/Seite** die maximale Anzahl von Elementen ein, die Sie auf den Seiten, die Paginierung verwenden, jeweils anzeigen möchten (die maximal zulässige Anzahl ist 500).
5. Um entlang der Schaltflächen auf den Symbolleisten Text anzuzeigen, aktivieren Sie das Kontrollkästchen **Text auf Symbolleisten anzeigen**.
6. Um sicherzustellen, dass es bei Ihrer aktiven Websitzung nicht zu einem Timeout kommt, wählen Sie

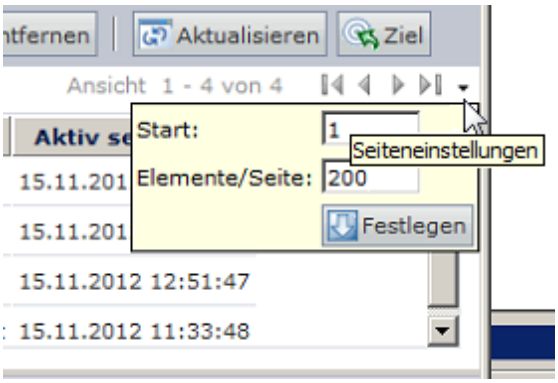
Websitzungen stets aufrecht erhalten.

7. Klicken Sie auf **Aktualisieren**.

HINWEIS: Sie können entlang der Schaltflächen auf den Symbolleisten Text einblenden, wodurch neuen Benutzern die Verwendung der Funktionen erleichtert wird. Wenn diese Option nicht ausgewählt ist, werden nur Symbole auf den Symbolleisten angezeigt. Für die Symbole wird jedoch Text eingeblendet, sobald der Mauszeiger auf sie gesetzt wird.

So zeigen Sie mehrere Geräte in der Ansicht einer Liste an

1. Klicken Sie in der Ansicht einer beliebigen Liste von Geräten ganz rechts (unterhalb der Symbolleiste) auf den Pfeil nach unten, um das Feld **Seiteneinstellungen** zu öffnen.



2. Geben Sie eine Zahl in das Feld **Elemente/Seite** ein (der Höchstwert ist 500).
3. Soll die Liste an einer weiter hinten liegenden Stelle als dem ersten Datensatz beginnen, ändern Sie den Zahlwert im Feld **Start**.
4. Klicken Sie auf **Festlegen**.

Ihre Änderungen sind nur wirksam, solange Sie in der aktuelle Liste arbeiten. Sobald Sie zu einer anderen Geräteliste wechseln, werden wieder so viele Geräte angezeigt, wie in der entsprechenden Einstellung auf der Registerkarte **Seiteneinstellungen** definiert wurden.

Konfigurieren von benutzerdefinierten Spalten [Webkonsole]

Verwenden Sie die Option **Benutzerdefinierte Spalten** zum Ändern von Spaltennamen und Feldern. Alle etwaigen Spaltenänderungen, die Sie vornehmen, sind für den Benutzer unsichtbar. Änderungen an benutzerdefinierten Spalten werden in der Ansicht **Eigene Geräte** angezeigt.

Die Webkonsole enthält einen Standardspaltensatz mit acht Spalten. Der Standardsatz lässt sich zwar nicht bearbeiten, Sie können jedoch einen benutzerdefinierten Spaltensatz als Ihren Standard-Spaltensatz verwenden.

HINWEIS: Es ist nicht zweckmäßig, benutzerdefinierte Spalten zu erstellen, die mehrere Feldnamen unterstützen. Beispiel: Wenn Sie ein "Computer.Software.Paket.Name"-Feld erstellen und auf dem Gerät mehrere Pakete installiert sind, listet Management Suite nur einen Paketnamen pro Zeile auf, selbst dann, wenn sich die anderen Paketnamen auf demselben Gerät befinden. Dies führt dazu, dass die Liste **Alle Geräte** mehrere Einträge für dasselbe Gerät anzeigen.

So erstellen Sie einen benutzerdefinierten Spaltensatz

1. Klicken Sie in der Toolbox der Webkonsole auf **Administration > Einstellungen**.
2. Klicken Sie auf der Registerkarte **Benutzerdefinierte Spalten** auf **Neu**.
3. Geben Sie einen Namen für den Spaltensatz ein.
4. Navigieren Sie im oberen Feld durch die Ordner, um das Attribut zu finden, das Sie für die jeweilige Spaltenüberschrift verwenden möchten. Wählen Sie ein Attribut aus und klicken Sie auf **Hinzufügen**.

   Das Feld enthält eine Ordnerstruktur, die mit **Computer** beginnt und alle derzeit in der Datenbank vorhandenen Inventardaten darstellt. Die einzelnen Attribute haben ein -Attributsymbol.

   HINWEIS: Wenn Sie ein Attribut in der Datenbank auswählen, das über eine 1:*-Beziehung verfügt, erhalten Sie Doppeleinträge für dieses Gerät. Wenn Sie Attribute mit einer 1:1-Beziehung auswählen (nur ein mögliches Attribut, z. B. Computer.System.Assetkennzeichen), erhalten Sie keine Doppeleinträge.

5. Um die Spaltenanordnung zu ändern, wählen Sie eine Spaltenüberschrift aus und klicken auf **Nach oben** oder **Nach unten**.
6. Um eine Spalte zu entfernen, wählen Sie sie aus und klicken auf **Entfernen**.
7. Um die für eine Spalte angezeigte Überschrift zu ändern, wählen Sie die Überschrift aus, klicken auf **Bearbeiten**, führen die gewünschten Änderungen durch und drücken die **Eingabetaste**. Die folgenden Zeichen des erweiterten Zeichensatzes werden nicht unterstützt: < , > , ' , " , !.
8. Klicken Sie auf **OK**, um den Spaltensatz zu speichern.
9. Um beim Anzeigen einer Geräteliste den benutzerdefinierten Spaltensatz zu verwenden, wählen Sie ihn aus und klicken in der Symbolleiste auf **Als aktuellen Spaltensatz auswählen**.

HINWEIS: Wenn Sie eine Oracle-Datenbank verwenden, wählen Sie mindestens ein Attribut aus, das direkt durch den Inventarscanner definiert ist (z. B. Computer.Anzeigename, Computer.Gerätename, Computer.Gerätekennung, Computer.Anmeldename usw.).

So bearbeiten Sie einen benutzerdefinierten Spaltensatz

1. Klicken Sie in der Toolbox der Webkonsole auf **Administration > Einstellungen**.
2. Klicken Sie auf die Registerkarte **Benutzerdefinierte Spalten**.
3. Wählen Sie den benutzerdefinierten Spaltensatz aus und klicken Sie auf **Bearbeiten**.
4. Folgen Sie beim Durchführen von Änderungen den Anweisungen in den Schritten 4 bis 8.
5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Tipps zur Fehlerbehebung

Die folgenden Tipps zur Fehlerkorrektur konzentrieren sich auf Probleme, die am häufigsten im Zusammenhang mit der Webkonsole auftreten.

Ich kenne die URL zur Webkonsole nicht.
Wenden Sie sich an die Person, die den Coreserver installiert hat, wahrscheinlich ist dies der Netzwerkadministrator Ihres Standorts. Die URL-Adresse lautet in der Regel http://*Computername des Coreservers*/remote.

Als welcher Benutzer bin ich angemeldet?
Sehen Sie in der Titelleiste nach. Der angemeldete Benutzer wird neben **Verbunden als:** angezeigt.

An welchem Gerät bin ich angemeldet?
Sehen Sie in der Titelleiste nach. Der Name des Coreservers wird neben **Verbunden mit:** angezeigt.

Ich sehe einige der Links in der Symbolleiste nicht.
Der Grund hierfür ist, dass Ihr Netzwerkadministrator die rollenbasierte Administration oder die Option für Sicherheit auf Funktionsebene verwendet und Sie dadurch auf bestimmte Tasks beschränkt werden, für die Sie Rechte besitzen.

Ich erhalte eine "Zugriff verweigert"-Fehlermeldung, wenn ich versuche, auf die Konsole zuzugreifen.
Für den Einsatz von Sicherheit auf Funktionsebene unter Windows 2000 und 2003 müssen Sie die anonyme Authentifizierung deaktivieren. Überprüfen Sie die Authentifizierungseinstellungen auf der Website und den Ordner..\LANDesk\ldsm unter der Website.

1. Klicken Sie auf dem Server, der die Webkonsole hostet, auf **Start > Verwaltung > Internet Information Services (IIS)-Manager**.
2. Klicken Sie im Kontextmenü der **Standardwebsite** auf **Eigenschaften**.
3. Klicken Sie auf der Registerkarte **Directory Security** im Abschnitt **Anonymer Zugriff und Authentifizierungskontrolle** auf **Bearbeiten**. Deaktivieren Sie die Option **Anonymen Zugriff aktivieren** und aktivieren Sie das Kontrollkästchen **Integrierte Windows-Authentifizierung**.
4. Klicken Sie auf **OK**, um die Dialogfelder zu schließen.
5. Klicken Sie vom Unterordner **landesk\managementsuite** der Standard-Website auf **Eigenschaften**. Wiederholen Sie die Schritte 3 - 4.

Ich erhalte eine ungültige Sitzung beim Anzeigen der Konsole.
Es kann sein, dass die Browser-Sitzung abgelaufen ist. Verwenden Sie die Schaltfläche **Aktualisieren** Ihres Browsers, um eine neue Sitzung zu starten.

Beim Versuch, die Webkonsole zu starten, wird ein ASP.NET-Fehler angezeigt.
Wenn beim Versuch der Anmeldung bei der Webkonsole eine ASP.NET-Fehlermeldung angezeigt wird, sind möglicherweise ASP und die ASP-Verzeichnisberechtigungen nicht korrekt konfiguriert. Setzen Sie die ASP.NET-Konfiguration zurück, indem Sie folgenden Befehl ausführen:

```
ASPNET_REGIIS.EXE -i
```

Die Anzahl der Objekte pro Seite stimmt nicht mit der von mir angegebenen Zahl überein.
Die Einstellung, mit der Sie angeben, wie viele Objekte pro Seite angezeigt werden sollen, wird im Cookie-Verzeichnis des Browsers gespeichert und wird deaktiviert, wenn das Sitzungstimeout der Konsolensitzung abläuft.

Das Sitzungstimeout für die Konsole läuft zu häufig ab.
Sie können das standardmäßige Sitzungstimeout für die Webseiten der Konsole ändern. Der IIS-Standard liegt bei 20 Minuten Inaktivität, bevor eine Anmeldung abläuft. So ändern Sie das IIS-Sitzungstimeout

1. Klicken Sie auf dem Webserver auf **Start > Verwaltung > Internetinformationsdienste (ISS)-Manager**.
2. Erweitern Sie die **Standardwebsite**.
3. Klicken Sie mit der rechten Maustaste auf den Ordner **LDMS** und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Virtuelles Verzeichnis** auf **Konfiguration**.
5. Klicken Sie auf die Registerkarte **Anwendungsoptionen** und ändern Sie das Sitzungstimeout in den gewünschten Wert.

HINWEIS: Management Suite ist ein sitzungsbasiertes Produkt. Deaktivieren Sie nicht den Sitzungsstatus.

Ich kann die Remotesteuerungsseite in der Webkonsole nicht anzeigen.
Um die Seite **Remotesteuerung** anzuzeigen, müssen Sie ActiveX-Controls aktivieren. Auf einigen Browsern sind ActiveX Controls standardmäßig deaktiviert. Wenn die Seite **Remotesteuerung** nicht ordnungsgemäß geladen wird, aktivieren Sie ActiveX Controls auf Ihrem Browser, indem Sie die Sicherheitseinstellungen ändern.

Ich habe den neuen Assistenten für die Softwareverteilung abgeschlossen, aber die Konsole hat kein Paket erstellt.
Die Konsole verwendet die IUSR- und IWAM-Konten auf Konsolenservern. Diese Konten werden ursprünglich auf der Basis des Computernamens erstellt. Wenn Sie den Computernamen irgendwann einmal geändert haben, müssen Sie die unten genannten Schritte ausführen, damit das Erstellen von Softwareverteilungspaketen klappt.

1. Wenn auf Ihrem System .Net Framework installiert ist, deinstallieren Sie es.
2. Deinstallieren Sie IIS.
3. Installieren Sie IIS neu.
4. Installieren Sie .Net Framework neu, wenn Sie es deinstalliert haben.

Ein geplanter Softwareverteilungsauftrag wurde nicht ausgeführt.
Wenn Sie einen Softwareverteilungsauftrag planen und dieser nicht ausgeführt wird, stellen Sie sicher, dass der Local Scheduler Service auf dem Gerät ausgeführt wird.

Beachten Sie darüber hinaus auch, dass die Planung des Jobs auf der Uhrzeit des Coreservers basiert. Wenn der Job auf einer Konsole geplant wurde, die sich in einer anderen Zeitzone befindet, wird der Job auf der Basis der Coreserver-Zeit gestartet, die ggf. nicht mit der erwarteten Zeit übereinstimmt.

Berichtsdiagramme werden nicht ordnungsgemäß angezeigt.
Damit die in vielen Berichten enthaltenen interaktiven Balken- und Tortendiagramme angezeigt werden, muss Adobe Flash Player installiert sein. Stellen Sie sicher, dass Flash installiert ist, und führen Sie dann den Bericht erneut aus.

Warum sehe ich zwei Instanzen desselben Geräts in meiner Datenbank?
Haben Sie ein Gerät aus der Coredatenbank gelöscht und mit "UninstallWinClient.exe" erneut installiert?

UninstallWinClient.exe befindet sich in der LDMain-Freigabe, dem Hauptprogrammordner von ManagementSuite. Nur Administratoren haben Zugriff auf diese Freigabe. Dieses Programm deinstalliert LANDesk Agenten auf jedem Gerät, auf dem es ausgeführt wird. Sie können es in jeden gewünschten Ordner verschieben oder zu einem Anmeldeskript hinzufügen. Es handelt sich dabei um eine Windows-Anwendung, die im Hintergrund ausgeführt wird, ohne eine Benutzeroberfläche einzublenden. Sie sehen möglicherweise zwei Instanzen des Geräts, das Sie gerade gelöscht haben, in der Datenbank. Eine dieser Instanzen enthält nur Protokolldaten, während die andere nach vorne gerichtete Daten enthält.

Ich habe ein S.M.A.R.T.-Laufwerk auf einem Gerät hinzugefügt, jedoch wird die S.M.A.R.T.-Laufwerksüberwachung für dieses Gerät in der Inventarliste nicht angezeigt.
Die Hardwareüberwachung ist von der Funktionalität der auf dem Gerät installierten Hardware sowie von der korrekten Konfiguration der Hardware abhängig. Wenn z.B. ein Festplattenlaufwerk installiert ist, das über S.M.A.R.T.-Überwachungsfunktionen verfügt, die S.M.A.R.T.-Erkennung jedoch nicht in den BIOS-Einstellungen des Geräts aktiviert ist, oder wenn das BIOS des Geräts keine S.M.A.R.T.-Laufwerke unterstützt, dann werden keine Überwachungsdaten bereitgestellt und auch keine resultierenden Alarme generiert.

In PXE-basierten OSD DOS-Skripten werden manche Teile nach dem Komma abgeschnitten
In Skriptzeilen werden alle Zeichen nach einem Komma abgeschnitten, sodass Befehle, die auf das Komma folgen, nicht ausgeführt werden. Umgehen Sie dies, indem Sie den gesamten Befehl wie folgt in doppelte Anführungszeichen setzen:

```
REMEXEC1=%QUOTE%echo "hi,good morning"%QUOTE%
```

Einfache Anführungszeichen funktionieren nicht, da sie beim Lesen der .INI-Datei extrahiert werden.

Beim Versuch, die Remotesteuerung von der Webkonsole aus in einem anderen Subnetz zu installieren, lässt sich der RC Viewer nicht installieren.
Wenn Sie eine Verbindung zu einer Webkonsole herstellen, die von einem Core in einer anderen Domäne gehostet wird, und Sie dann mit der rechten Maustaste auf einen Computer in der Liste **Eigene Geräte** klicken und **Remotesteuerung** auswählen, erhalten Sie eine Fehlermeldung, die besagt, dass der RC Viewer nicht ordnungsgemäß installiert wurde.

Die URL für die CAB-Datei ergibt sich durch Auslesen des Kennzeichens mit dem Namen "CabUrl" aus web.config. Das Kennzeichen CabUrl muss den vollständig qualifizierten Domänennamen des Cores enthalten. Der Computername alleine reicht nicht. Sie müssen "web.config" öffnen und den vollständig qualifizierten Domänennamen in das CabUrl-Tag einfügen.

Ein USB-Datenträgergerät wird erst in der Inventarliste angezeigt, nachdem ein Inventarscan ausgeführt wurde.
Wenn ein Datenträgergerät mit einem USB-Kabel an ein verwaltetes Gerät angeschlossen ist, wird es nicht sofort unter "Festplattenlaufwerke" im Inventar des Geräts aufgeführt. Es wird unter "Logische Laufwerke" aufgelistet, nachdem es mit dem Gerät verbunden wurde. Es wird erst unter "Festplattenlaufwerke" angezeigt, nachdem ein Inventarscan auf dem Gerät ausgeführt wurde.

Auf verwalteten Linux-Geräten muss ein USB-Datenträgergerät gemountet werden, damit es im Inventar aufgelistet wird. Wenn es gemountet wird, aber noch kein Inventarscan ausgeführt wurde, wird es unter "Logische Laufwerke" angezeigt; nach Ausführung des Inventarscans wird es auch unter "Festplattenlaufwerke" angezeigt. Wenn das Gerät getrennt wird, sollte es aus dem System deaktiviert (Dismounting) werden. Auf einigen Linux-Systemen, die einen älteren Kernel ausführen, verbleibt das Gerät u.U. in der Liste, selbst nachdem es getrennt und deaktiviert wurde. In diesem Fall muss das verwaltete Gerät neu gebootet werden, damit es aus der Inventarliste gelöscht wird.

In der Liste "Alle Geräte" wird zweimal dieselbe IP-Adresse angezeigt
Für Linux-Geräte, die sich auf einem anderen Segment als der Core befinden, erhalten Sie möglicherweise mehrere Einträge mit identischer IP-Adresse in der Liste "Eigene Geräte". Für Knoten, die sich im selben Netzwerksegment wie der Core befinden, extrahiert die Erkennung die MAC-Adresse eines Knotens aus dem Ethernet (aus dem ICMP-Paket). Für Knoten, die sich nicht im selben Netzwerksegment wie der Core befinden, extrahiert die Erkennung die MAC-Adresse aus einer NETBIOS-Abfrage. Da Linux-Knoten nicht auf NETBIOS-Abfragen reagieren, kann eine MAC-Adresse für Linux-Knoten, die sich in einem anderen Netzwerksegment befinden als der Core, nicht über eine standardmäßige Netzwerkscan-Erkennung ermittelt werden. Wenn ein Client auf einem Knoten bereitgestellt wird, wird die MAC-Adresse in der Scandatei dazu verwendet, den zu aktualisierenden Inventardatensatz ausfindig zu machen (nachdem ein Versuch mit der DeviceID unternommen wurde). Datensätze ohne MAC-Adresse und DeviceID werden nicht gefunden, sodass ein neuer Datensatz erstellt wird. Sie können den doppelt vorhandenen Eintrag in der Liste "Erkannte Geräte" löschen.

Anzeigen der Echtzeitinventar- und Überwachungskonsole [Webkonsole]

Mit der Echzeitinventar- und Überwachungskonsole können Sie Übersichtsdaten zu einem Gerät sowie Systeminformationen wie CPU- oder Lüfterdaten anzeigen, den Serverzustand und Grenzwerte wichtiger Gerätebestandteile überwachen, Anfälligkeiten verwalten sowie ein Gerät ein- oder abschalten und neu starten.

Die Echzeitinventar- und Überwachungskonsole umfasst die folgenden Extras:

- Systeminformationen
- Remotesteuerungssitzung
- Überwachung
- Regelsätze
- Stromoptionen
- Hardwarekonfiguration

HINWEIS: Um die Echzeitinventar- und Überwachungskonsole für ein Gerät anzuzeigen, müssen Sie zunächst den LANDesk Management-Agenten mit ausgewählten Echzeitinventar- und

Überwachungskomponenten auf dem Gerät bereitstellen. Außerdem muss das Gerät nach Installation des Agenten neu gestartet werden, damit die Serverinformationskonsole richtig funktioniert. Ein Neustart ist bei Installation von Agenten sowohl auf dem Coreserver als auch auf verwalteten Geräten erforderlich.

So zeigen Sie die Echtzeitinventar-Konsole an

1. Klicken Sie in der Management Suite Konsole mit der rechten Maustaste auf das verwaltete Gerät und wählen Sie **Echtzeitinventar und Überwachung** aus.

   Sie können auch auf **Extras > Berichte/Überwachung > Health Dashboard** klicken und anschließend in der Liste der Geräte auf ein Gerät doppelklicken.

   Die Konsole wird in einem neuen Browserfenster geöffnet und zeigt in der Grundeinstellung die Seite **Zustand – Übersicht** an.

2. Klicken Sie auf die Schaltflächen "Zustand – Übersicht", um detaillierte Informationen zum Gerätezustand abzurufen.
3. Klicken Sie auf die Elemente in der Toolbox, um die verfügbaren Extras zu verwenden.

Systeminformationen

Systeminformationen enthält eine Zusammenfassung des Systemzustands sowie Informationen über Hardware und Software, Systemprotokolle und andere Daten wie Informationen zu den vorhandenen Geräten und zum Netzwerk.

Zustand – Übersicht

Die Seite **Zustand – Übersicht** gibt eine schnelle Übersicht über den Systemzustand des jeweiligen Geräts. Sie erkennen auf einen Blick, ob die ausgewählten Hardwareelemente wie vorgesehen arbeiten oder ob sich Probleme abzeichnen, denen Sie ggf. Aufmerksamkeit schenken müssen.

Wenn sich einer der Systemfaktoren in einem Warn- oder kritischen Zustand befindet, wird in der zugehörigen Schaltfläche ein gelbes (Warnung) oder rotes (kritisch) Symbol eingeblendet, das auf das Problem hinweist. Klicken Sie auf die Schaltfläche, um eine Beschreibung des auslösenden Ereignisses anzuzeigen.

System – Übersicht

Verwenden Sie die Seite **System Übersicht**, um wichtige Informationen zum ausgewählten Gerät anzuzeigen. Die angegebenen Informationen können Folgendes umfassen, je nach Hardware- und Softwarekonfiguration des Geräts:

- **Zustand:** Der Gesamtzustand des Geräts gemäß den von Ihnen festgelegten Bedingungen und Parametern.
- **Typ:** Der Gerätetyp, beispielsweise Druck-, Programm- oder Datenbankserver.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Das Gerätemodell.
- **BIOS-Version:** Die BIOS-Version des Geräts.
- **Betriebssystem:** Das Betriebssystem des Geräts.
- **Betriebssystemversion:** Die Versionsnummer des Betriebssystems.
- **CPU:** Hersteller, Modell und Geschwindigkeit des Geräteprozessors.

- **IPMI-Typ, IPMI-Version:** Die vom Gerät verwendete IPMI-Version und IPMI-Typ.
- **BMC-Version:** Bei Intel AMT- und vPro-Geräten ist dies die Versionsnummer des Baseboard Management Controllers.
- **SDR-Version:** Die Version des Sensordatensatzes im BMC des Geräts.
- **Anfälligkeitsscanner:** Die Version des Anfälligkeitsscanners.
- **Remotesteuerung:** Die Version des Remotesteuerungsagenten.
- **Softwareverteilung:** Die Version des Softwareverteilungsagenten.
- **Inventarscanner:** Die Version des Inventarscanners.
- **Kern:** Bei Linux-Geräten die Versionsnummer des installierten Kerns.
- **Überwachung:** Die Versionsnummer des Überwachungsagenten auf dem Gerät.
- **CPU-Nutzung:** Prozentsatz des derzeit verwendeten Prozessors.
- **Physikalischer Speicher verwendet*:** Der Prozentsatz des insgesamt auf dem Gerät verwendeten physikalischen Speichers.
- **Virtueller Speicher verwendet*:** Der Prozentsatz des insgesamt auf dem Gerät verwendeten virtuellen Speichers.
- **Letzter Neustart*:** Datum und Uhrzeit des letzten Geräte-Neustarts (in der Zeitzone der Datenbank).
- **Laufwerk:** Die Laufwerke auf dem Gerät unter Angabe der Gesamtgröße des Laufwerks und des Prozentsatzes an verwendetem Speicher.

Diese Informationen werden aus der Registrierung in Windows oder aus den Konfigurationsdateien in Linux abgerufen.

*Diese Informationen werden angezeigt, nachdem ein Agent auf dem Gerät installiert wurde.

Hardware

Verwenden Sie die Seite **Hardware**, um Details zur Hardwarekonfiguration des Geräts anzuzeigen. Die Einträge in der Liste **Hardware** sind nach folgenden Kategorien gruppiert. Nicht alle Kategorien werden für alle Geräte angezeigt. Wenn das Gerät z. B. keinen Lüfter und keine Temperatursensoren hat, erscheint die Kategorie **Kühlung** nicht in dieser Liste.

- **CPU:** Prozessoren und Cache
- **Speicher:** Logische Laufwerke, physikalische Laufwerke, mobile Medien und Speicheradapter
- **Speicher:** Speichernutzung und Speichermodule
- **Gehäuse:** Das Gehäuse des Servers; Anzeige, ob das Gehäuse offen oder geschlossen ist
- **Eingabegeräte:** Tastatur, Maus und andere Geräte
- **Motherboard:** Motherboard, Steckplätze und BIOS
- **Kühlung:** Lüfter und Temperatursensoren
- **FRUs:** FRUs (Field-replaceable units)
- **Strom:** Stromversorgung
- **Spannung:** Spannungswerte
- **IPMI-Sensoren:** Diskrete und numerische Sensoren
- **Dell DRAC:** Dell DRAC-Daten. Klicken Sie auf Schaltfläche, um das Dell DRAC-Dienstprogramm und den Dell DRAC-Serveradministrator zu starten.

Einstellen von Warngrenzwerten für Hardwarekomponenten

Einige Komponenten in der Liste **Hardware** enthalten Daten von Sensoren im Gerät, wie z. B. Temperatursensoren. Wenn ein verwaltetes Gerät über Komponenten mit unterstützten Sensoren verfügt, können Sie die Sensormesswerte ändern, die einen Alarm auslösen. So kann z. B. für den CPU-Temperatursensor bei Unter- bzw. Überschreitung bestimmter Messwerte eine Warnmeldung oder kritischer Alarm ausgelöst werden. Die Grenzwerte richten sich in der Regel nach den vom Hersteller empfohlenen Einstellungen, Sie können jedoch die oberen und unteren Grenzwerte im Dialogfeld **Grenzwerte** ändern.

1. Klicken Sie in der Toolbox **Echtzeitinventar und Überwachung** auf **Systeminformationen**.
2. Erweitern Sie den Ordner **Hardware** und suchen Sie das gewünschte Hardwareelement (z. B. **Kühlung > Temperaturen**).
3. Doppelklicken Sie in der Liste der Sensoren auf den Sensor, dessen Grenzwerte Sie ändern möchten.
4. Geben Sie die gewünschten Werte in die Textfelder für den unteren und/oder oberen Grenzwert ein oder ziehen Sie die Schieberegler auf dem Trackbar nach links oder rechts, um die Werte zu ändern.
5. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen zu speichern.
6. Klicken Sie zum Wiederherstellen der ursprünglichen Grenzwerte auf **Standardeinstellungen wiederherstellen**.

Protokolle

Die Seite **Protokolle** zeigt die lokalen Systemprotokolle, das System Events Log (SEL) für IPMI-Geräte und ein Alarmprotokoll an.

Lokale Protokolle, wie beispielsweise die Protokolle **Anwendung**, **Sicherheit** und **System** weisen eine Schaltfläche **Aktualisieren** auf, mit der die aktuellsten Daten angezeigt werden können, und eine Schaltfläche **Löschen**, mit der sämtliche Elemente aus der Liste gelöscht werden können.

Wenn das Geräte-BIOS über die Funktionalität zum Löschen des **BIOS**-Protokolls verfügt, klicken Sie auf die Schaltfläche **Löschen**, um alle Protokolleinträge zu entfernen. Diese Schaltfläche ist nicht verfügbar, wenn dieser Vorgang vom BIOS nicht unterstützt wird.

Das **Alarm**protokoll zeigt alle aktuellen Alarme für das Gerät an. Sie können nach Name, Status oder Instanz filtern, wenn Sie die Anzahl der Alarme in der Liste reduzieren möchten, und Sie können den Datumsfilter aktivieren, um nur Alarme für einen bestimmten Datumsbereich anzuzeigen.

Das Protokoll **Hardwareereignisse** zeigt Echtzeitdaten oder archivierte Elemente an. Sie können einzelne Elemente löschen, sämtliche Elemente in der Liste löschen oder die Liste aktualisieren, um die neuesten Protokollelemente anzuzeigen.

Die Seite **Versorgungsverlauf** zeigt den Versorgungsverlauf für das Gerät an, einschließlich Datum der Versorgungsaktion, deren Status und die verwendete Vorlage.

Software

Die Seite **Software** zeigt zusammenfassende Informationen über Prozesse, Dienste und Pakete auf dem jeweiligen Gerät an sowie eine Liste der aktuellen Umgebungsvariablen.

- **Prozesse:** Zeigt die laufenden Prozesse an. Klicken Sie mit der rechten Maustaste auf einen Prozess und wählen Sie **Prozess beenden**, um ihn zu beenden.
- **Dienste:** Zeigt die auf dem Gerät verfügbaren Dienste sowie deren Status an. Klicken Sie mit der rechten Maustaste auf einen Dienst und wählen Sie dann **Stopp**, **Start** oder **Neu starten**, um Änderungen vorzunehmen.

- **Pakete:** Gibt die installierten Pakete mit Versionsnummern und Namen der Lieferanten an.
- **Umgebung:** Führt die derzeit für das Gerät eingestellten Umgebungsvariablen auf.

Sonstige

Die Seite **Sonstige** enthält Inventarinformationen sowie eine Zusammenfassung der Netzwerk-Hardware und -Verbindungen.

- **Assetinformationen:** Dient zur Anzeige und zum Bearbeiten von Assetinformationen. Klicken Sie auf **Kontaktinformationen**, um Einzelheiten, wie beispielsweise den Namen und die Position der Person einzugeben, die das Gerät verwendet, sowie den Standort, die Abteilung und die Nummer des Assetkennzeichens auf dem Gerät. Klicken Sie auf **Systeminformationen**, um die Systeminformationen wie beispielsweise die Seriennummer, den Hersteller und den Gehäusetyp anzuzeigen.
- **Netzwerkinformationen:** Anzeige einer Liste der installierten Netzwerk-Hardware, der Statistiken für die Netzwerkaktivität, einer Konfigurationsübersicht (einschließlich IP-Adresse, Standard-Gateway-Adresse sowie WINS-, DHCP- und DNS-Serverinformationen) und einer Liste der aktuellen Netzwerkverbindungen (zugeordnete Laufwerke)

Remotesteuerungssitzung

Verwenden Sie **Remotesteuerungssitzung**, um eine Remotesteuerungssitzung mit dem ausgewählten Gerät zu starten. Wenn das Gerät ein Windows-Server ist, wird die Standard-Remotesteuerung des Produkts gestartet. Für Linux-Server können Sie zwischen SSH- und SFTP-Sitzungen wählen.

Klicken Sie in der Toolbox **Echtzeitinventar und Überwachung** auf **Remotesitzung** und klicken Sie dann auf **Starten**, um die Remotesteuerungssitzung zu initiieren.

Überwachung

Verwenden Sie die **Überwachung** zur Anzeige von Leistungszählern und zum Definieren von Grenzwerten für Gerätekomponenten. Leistungszähler werden mit dem Alarm **Leistungsüberwachung** verwendet, um bestimmte leistungsbezogene Ereignisse eines Geräts zu überwachen. Auf dem Gerät muss ein Alarmregelsatz bereitgestellt sein, der die Alarmregel Leistungsüberwachung enthält, damit es Alarme aufgrund der Leistungszähler empfangen kann.

So wählen Sie einen zu überwachenden Leistungszähler aus

1. Klicken Sie in der Toolbox **Echtzeitinventar und Überwachung** auf **Überwachung**.
2. Klicken Sie auf die Registerkarte **Einstellungen für die Leistungszähler**.
3. Wählen Sie in der Spalte **Objekte** das zu überwachende Objekt aus.
4. Wählen Sie in der Spalte **Instanzen** ggf. die Instanz des zu überwachenden Objekts aus.
5. Wählen Sie in der Spalte **Zähler** den zu überwachenden Zähler aus.
6. Geben Sie das Abfrageintervall an und die Anzahl von Tagen, die der Zählerverlauf gespeichert werden soll.
7. Geben Sie im Textfeld **Alarmieren, sobald Zähler außerhalb des gültigen Bereichs liegt** an, wie oft der Zähler die Grenzwerte überschreiten darf, ehe ein Alarm generiert wird.
8. Geben Sie die unteren und/oder oberen Grenzwerte an.
9. Klicken Sie auf **Übernehmen**.

So zeigen Sie das Leistungsdiagramm für einen überwachten Zähler an

1. Klicken Sie auf die Registerkarte **Aktive Leistungszähler**.
2. Wählen Sie in der Dropdownliste **Zähler** den Zähler aus, für den Sie ein Leistungsdiagramm anzeigen möchten.
3. Wählen Sie **Echtzeitdaten anzeigen**, um ein Diagramm der derzeitigen Leistung einzublenden. Oder wählen Sie **Vergangenheitsdaten anzeigen** aus, um ein Diagramm einzublenden, das über die Leistung Auskunft gibt, die während des Zeitraums erzielt wurde, den Sie beim Auswählen des Zählers (mit der Option **Verlauf speichern**) festgelegt hatten).

Im Leistungsdiagramm repräsentiert die Horizontalachse den verstrichenen Zeitraum. Die Vertikalachse repräsentiert die gemessenen Einheiten, beispielsweise Byte/Sek. (beim Überwachen von Dateiübertragungen), Prozent (beim Überwachen des Prozentsatzes der CPU-Nutzung) oder verfügbare Byte (beim Überwachen des Festplattenspeichers).

Regelsätze

Das Extra **Regelsätze** verwenden Sie, um eine Liste mit den Alarmregelsatzkonfigurationen anzuzeigen, die dem ausgewählten Gerät zugewiesen wurden; Sie können mit dieser Seite auch detaillierte Informationen zu den einzelnen Alarmen anzeigen.

So zeigen Sie Alarmregelsätze an

1. Klicken Sie in der Toolbox **Echtzeitinventar und Überwachung** auf **Regelsätze**.
2. Wählen Sie einen Regelsatznamen aus der Dropdownliste aus, um die Details dieses Regelsatzes anzuzeigen.

Die Spalten für jeden Alarm werden nachstehend beschrieben.

- **Alarmtyp:** Eine Beschreibung des überwachten Alarmereignisses.
- **Status:** Wenn ein Alarmereignis den Schwerezustand in dieser Spalte erreicht, wird ein Alarm ausgelöst. Sie können mehrere Zustände für ein Ereignis auswählen.
- **Aktion:** Die Aktion, die abläuft, wenn der Alarm generiert wird (entsprechend der Definition des Alarmregelsatzes).
- **Zum Zustand hinzufügen:** Wenn das Alarmereignis den angegebenen Zustand erreicht, ändert sich der Gerätezustand in der Liste **Alle Geräte** oder dem Health-Dashboard.

Stromoptionen

Mit den **Energieoptionen** können Sie Remotegeräte abschalten, neu starten und (im Falle verwalteter IPMI und Intel vPro-Geräte) einschalten. Bei Nicht-IPMI-Servern muss auf dem Gerät der LANDesk Agent bereitgestellt worden sein, damit die Neustart- und Abschaltfunktionen ausgeführt werden können.

Bei IPMI und Intel vPro-Geräten müssen Sie über die korrekten Anmeldeinformationen verfügen, um die Einschalt-/Abschalt- und Neustartfunktionen ausführen zu können. Wenn auf IPMI- oder Intel vPro-Geräten der LANDesk Agent bereitgestellt wurde, können Sie die Abschalt- und Neustartfunktionen ohne die IPMI- oder Intel vPro-Anmeldeinformationen durchführen. Zum Konfigurieren von BMC-Anmeldeinformationen für IPMI-Geräte verwenden Sie die Funktion "Dienste konfigurieren".

So verwenden Sie die Stromoptionen auf dem ausgewählten Gerät

1. Klicken Sie in der Toolbox **Echtzeitinventar und Überwachung** auf **Energieoptionen**.
2. Wählen Sie **Neu starten**, **Ausschalten** oder **Einschalten** und klicken Sie dann auf **Senden**.

HINWEIS: Wenn Sie mehrere Coreserver besitzen, können Sie Stromoptionen nur von dem Coreserver aus verwenden, bei dem Sie sich zuerst anmelden. Wenn Sie zu einem anderen Core wechseln und dann versuchen, die Stromoptionen zu verwenden, schlägt der Strombefehl fehl.

Hardwarekonfiguration

Mit dem Extra **Hardwarekonfiguration** können Sie Optionen für Geräte mit IPMI, Intel vPro und Dell DRAC-Funktionen konfigurieren. Dieses Tool und die Optionen werden nur bei Geräten angezeigt, die über die entsprechende Hardware verfügen (Beispiel: IPMI-Optionen werden nur angezeigt, wenn das Gerät als IPMI-Gerät erkannt wird).

Verwenden des Health Dashboards [Webkonsole]

Das Health Dashboard ist ein einfacher übersichtlicher Bildschirm, auf dem Ihre Geräte angezeigt werden. Es zeigt für jedes Gerät ein Symbol an, dessen Farbe den aktuellen Zustand des Geräts verdeutlicht. Die im Health Dashboard angezeigten Geräte basieren auf Bereichen und Rollen. Das Health Dashboard lässt sich verschieben und konfigurieren. Es gibt Auskunft über den Gesamtzustand der in der Übersicht dargestellten Geräte, wobei die Geräte nach Zustand sortiert sind (X Geräte in einem kritischen Zustand, X Geräte in einem normalen Zustand usw.). Sie können ein Diagramm und eine Geräteliste einblenden oder die Verankerung des Diagramms aufheben, um es nur für sich auf Ihrer Arbeitsstation oder einem Gruppenbildschirm anzeigen.

Wenn Sie mit der rechten Maustaste auf das Symbol eines Geräts klicken, können Sie Basiselemente für die Problembehandlung auswählen wie Ping, Trace Route und Remotesteuerung (wenn das Gerät ein verwaltetes Gerät ist). Sie können auch **Details anzeigen** wählen, um die Echtzeitinventar- und Überwachungskonsole aufzurufen.

- So öffnen Sie das Health Dashboard
- So zeigen Sie die Echtzeitinventar-und Überwachungskonsole an
- So zeigen Sie Geräteeigenschaften an
- So beheben Sie einfache Fehler
- So sortieren Sie Geräte nach Namen oder Zustand
- So verankern Sie das Health Dashboard-Diagramm
- So zeigen Sie Geräte nach Statuskategorie an
- So aktualisieren Sie das Health Dashboard

So öffnen Sie das Health Dashboard

1. Klicken Sie in der LANDesk Management-Konsole auf **Extras > Berichte / Überwachung > Health Dashboard**.

   Das Health Dashboard wird in einem Webbrowser geöffnet. Es zeigt die Geräte an, die in der Gruppe **Alle Geräte** aufgeführt sind. Wenn Geräte mehrmals in der Liste **Alle Geräte** aufgeführt sind, werden sie mehrmals im Health Dashboard aufgelistet.

2. So verhindern Sie, dass Geräte mehrmals aufgeführt werden:
    - Konfigurieren Sie die Optionen für die Handhabung doppelter Gerätenamen über das Dialogfeld **LANDesk Softwaredienste konfigurieren**. (Klicken Sie in der LANDesk Management Console auf **Konfigurieren > Dienste**.)
    - Wählen Sie beim Anpassen von Spalten in der Geräteansicht nach Möglichkeit kein Attribut aus, das dazu führt, dass ein Gerät mehrmals aufgelistet wird. Beispiel: Das Auswählen von Softwareanwendungen kann zur Folge haben, dass ein Gerät mehrmals in der Liste angezeigt wird, da es pro einzelner installierter Softwareanwendung einmal aufgeführt wird.

HINWEIS: Damit Dialogfelder und Fenster ordnungsgemäß angezeigt werden, muss der Management Suite Webserver zur Liste "Zugelassen" im Popupblocker des Browsers hinzugefügt werden.

So zeigen Sie die Echtzeitinventar-und Überwachungskonsole an

- Doppelklicken Sie im Health Dashboard auf ein Gerät.

In der Echtzeitinventar und Überwachungskonsole sind wesentliche Inventar- und Systeminformationen aufgeführt, sowie die Remotesteuerungsoption, die Einstellungen für die Alarmierung und Leistungsüberwachung und die Energieoptionen.

Nähere Informationen finden Sie unter "Anzeigen der Echtzeitinventar- und Überwachungskonsole [Webkonsole]" auf Seite 950.

So zeigen Sie Geräteeigenschaften an

- Klicken Sie im Health Dashboard mit der rechten Maustaste auf ein Gerät und klicken Sie dann auf **Eigenschaften**.

Sie können den Gerätenamen, die IP-Adresse, den Prozentsatz der CPU- und Speichernutzung und den verfügbaren Festplattenspeicher anzeigen. Durch das Anzeigen von **Eigenschaften** wird eine Verbindung zum betreffenden Gerät hergestellt, um Echtzeitdaten zu zentralen Messgrößen wie Speicherplatz und verbrauchter Speicher zu sammeln.

Ist das Gerät offline (oder nicht in der Lage, über das Netzwerk zu kommunizieren), meldet das Dialogfeld **Eigenschaften** einen Fehler.

HINWEIS: Wurde die Option **Echtzeitinventar und Überwachung** nicht mit dem LANDesk Agenten auf einem Gerät installiert, wird die Option **Eigenschaften** beim Rechtsklick auf das Gerät nicht angezeigt.

So beheben Sie einfache Fehler

Das Health Dashboard bietet Funktionen zur Fehlerdiagnose und -beseitigung, beispielsweise Geräteping, Remotesteuerung (sofern das Gerät verwaltet ist) und Zugriff auf die Geräteinformationskonsole eines Geräts.

1. Um ein Gerät per Remotesteuerung zu bedienen, klicken Sie mit der rechten Maustaste auf das Gerät und wählen **Remotesteuerung**.
2. Um ein Gerät mit einem Pingsignal zu testen, klicken Sie mit der rechten Maustaste auf das Gerät und wählen **Einen Pingtest mit dem Gerät durchführen**.
3. Um einen Trace-Route-Befehl an ein Gerät zu senden, klicken Sie mit der rechten Maustaste auf das Gerät und wählen **Einen Traceroutetest mit dem Gerät durchführen** aus.

So sortieren Sie Geräte nach Namen oder Zustand

1. Klicken Sie in der Symbolleiste des Health Dashboards auf die Dropdownliste **Sortieren nach**.
2. Wählen Sie entweder **Name** oder **Zustand**.

So verankern Sie das Health Dashboard-Diagramm

1. Klicken Sie in der Symbolleiste des Health Dashboards auf **Diagramm andocken**.

   Daraufhin wird ein verankerbares Fenster geöffnet, das das Diagramm und grundlegende Statusinformationen anzeigt.

2. Möchten Sie das Diagramm wieder in das Hauptfenster des Health Dashboard zurückstellen, klicken Sie nochmals auf die Schaltfläche **Diagramm andocken**.

So zeigen Sie Geräte nach Statuskategorie an

1. Klicken Sie in der Symbolleiste des Health Dashboards auf die Dropdownliste **Anzeigen**.
2. Wählen Sie eine Option für den Zustand (Normal, Warnung, Kritisch oder Alle).

HINWEIS: Sie können auch auf einen Balken (oder einen Tortenausschnitt) im Diagramm klicken, um nur die Geräte anzuzeigen, die diesem Status entsprechen.

So aktualisieren Sie das Health Dashboard

Nachdem Sie neue Geräte zur Liste **Eigene Geräte** hinzugefügt haben, müssen Sie das Health Dashboard manuell aktualisieren, damit diese neuen Geräte angezeigt werden. Hierzu klicken Sie auf die Schaltfläche **Aktualisieren** in der Symbolleiste des Health Dashboards.

Damit können Sie Geräte zur Liste hinzufügen bzw. aus ihr entfernen und den Status eines jeden Geräts aktualisieren. Es ist nicht erforderlich, das Health Dashboard manuell zu aktualisieren, um den aktuellen Gerätezustand anzuzeigen. Wenn sich der Zustand eines überwachten Geräts ändert, aktualisiert das Health Dashboard automatisch seine Gerätesymbole, um den aktuellen Gerätezustand wiederzugeben.

Konfigurieren von Health-Dashboard-Optionen [Webkonsole]

So konfigurieren Sie die Anzeige von Daten im Health Dashboard

1. Klicken Sie in der Symbolleiste des Health-Dashboards auf die Schaltfläche **Optionen**.
2. Geben Sie eine Zahl (in Sekunden) in das Feld **Aktualisieren alle** ein, um festzulegen, wie oft das Health-Dashboard Zustandsaktualisierungen abfragen soll.
3. Wählen Sie im Listenfeld **Diagrammtyp** den gewünschten Diagrammtyp aus (3D-Balken, 3D-Kreis, 2D-Balken, 2D-Kreis).
4. Wählen Sie im Listenfeld **Anzeigen** die Statuskategorie aus, die Sie anzeigen möchten. Sie können alle Geräte oder nur einem bestimmten Statustyp (unbekannt, Warnung, kritisch, kritisch/Warnung) zugeordnete Geräte anzeigen.
5. Geben Sie an, wie die Geräte sortiert werden sollen (nach Name oder Zustand).
6. Wählen Sie **Große Symbole**, damit in der Health-Dashboard-Ansicht große Symbole angezeigt wird.

7. Wählen Sie **Listenansicht** aus, um die Geräte mit denselben Spalten wie die Hauptkonsole anzuzeigen. In dieser Ansicht werden keine großen Symbole angezeigt.
8. Klicken Sie auf **OK**.

Der Zustandsstatus wird entsprechend der von Ihnen in diesem Dialogfeld definierten Frequenz aktualisiert. Wenn Sie den Status sofort aktualisieren möchten, können Sie in der Symbolleiste auf die Schaltfläche **Aktualisieren** klicken.

Verwenden der Remotesteuerung [Webkonsole]

Mit der Remotesteuerung können Sie Geräteprobleme diagnostizieren und beheben. Während einer Remotesteuerungssitzung können Sie jeden Vorgang auf einem Remotecomputer ausführen, den ein Benutzer der direkt davor sitzt, ausführen könnte, wobei sie jedoch das Tastaturlayout Ihres Computers verwenden. Alle Aktionen werden in Echtzeit auf dem betreffenden Computer ausgeführt. Die Remotesteuerung ermöglicht Ihnen:

- Schnelles Beheben und Erkennen von Software- und Hardwareproblemen, indem sie es autorisierten Benutzern gestattet, einen Computer von einem entfernten Standort aus zu überprüfen und zu steuern
- Zugriff auf Remotedateien
- Übertragen von Dateien in beide Richtungen
- Ausführen von Remoteanwendungen
- Remoteneustart

Den Remotesteuerungszugriff für Benutzer richten Sie über das Extra für die rollenbasierte Administration ein. Wenn Sie mit integrierter oder zertifikatsbasierter Sicherheit arbeiten, kann das Remotesteuerungsrecht so konfiguriert werden, dass bestimmte Wochentage und/oder Tageszeiten ausgeschlossen werden. Wenn ein Benutzer einen Computer über eine Fernverbindung steuert und dem Remotesteuerungsrecht dieses Benutzers eine Zeitbeschränkung hinzugefügt wurde, ist die Sitzung nach Erreichen der Ablaufzeit der Beschränkung nicht mehr funktionsfähig.

Voraussetzungen für die Verwendung der Remotesteuerung

- Um die Remotesteuerung über die Konsole einzusetzen, müssen Sie zunächst den Remote Control Viewer installieren. Sie benötigen administrative Rechte auf dem lokalen Computer, um den Viewer zu installieren. Wenn Sie die Remotesteuerungsseite zum ersten Mal aufrufen, werden Sie aufgefordert, den Viewer zu installieren. Falls erforderlich, können Sie den Remote Control Viewer über die Systemsteuerung von Windows und den Befehl zum Hinzufügen/Entfernen von Programmen deinstallieren. Suchen Sie in der Programmliste nach **LANDeskManagement Suite Remotesteuerungskonsole**.
- Damit Windows-Geräte remote bedient werden können, muss auf ihnen der Remotesteuerungsagent des Produkts installiert und geladen sein. Dieser Agent wird durch eine der folgenden Aktionen installiert:
    - Erstellen eines Agentenkonfigurationstasks in der Konsole und Planen der Bereitstellung für das Gerät
    - Zuordnen eines Laufwerks auf dem Gerät zum Coreserver und Ausführen der entsprechenden Agentenkonfiguration

  Dieser Agent kann als residenter Dienst geladen werden, um direkten Zugriff auf den Computer zu ermöglichen, oder er kann (wenn Sie über zertifikatsbasierte Sicherheit verfügen) als Agent auf Abruf installiert werden, der nur geladen wird, wenn Bedarf besteht.

- Zusätzlich können Sie den Remotesteuerungsspiegeltreiber installieren, um die Leistung beim Erkennen, Aufzeichnen und Komprimieren von Bildschirmänderungen zu verbessern, wenn die Geräte-CPU langsam (< 2,0 GHz) oder das Netzwerk schnell ist (> 100 MBps). Beachten Sie, dass die Remotesteuerung keine DOS-Grafiken oder DOS-Ganzbildfenster unterstützt. Das Eingabeaufforderungsfenster wird zunächst möglicherweise nicht angezeigt, wenn der Spiegeltreiber verwendet wird. Ist dies der Fall, minimieren Sie das Fenster und maximieren Sie es anschließend.

Verwenden der Remotesteuerung

So steuern Sie ein Gerät remote über die Webkonsole

1. Klicken Sie in einer beliebigen Liste **Eigene Geräte** auf das Symbol des Geräts, zu dem Sie eine Verbindung herstellen möchten und wählen Sie **Remotesteuerung**.

   Alternativ können Sie auch das Gerät auswählen und im Aktionsbereich auf **Einstellungen > Remotesteuerung** klicken.

   Mit dieser Aktion wird der LANDesk Remote Control Viewer geöffnet. KVM-Remotesteuerung für Intel vPro-Geräte und eine browsergestützte HTML 5-Remotesteuerung sind weitere Remotesteuerungsoptionen.

2. Wenn Sie eine andere Art der Remotesteuerung bevorzugen, klicken Sie in der Toolbox der Webkonsole auf **Remotezugriff > Remotesteuerung**. Wählen Sie **Direkt**, **KVM** oder **Browser-gestützt** aus und geben Sie den Gerätenamen oder die IP-Adresse des Geräts an, das Sie steuern möchten.

Außerdem können mehrere Computer gleichzeitig ferngesteuert werden. Kehren Sie zur Webkonsole zurück, nachdem Sie eine Sitzung gestartet haben, und wählen Sie einen weiteren Computer aus.

Informationen zur Remotesteuerung von Linux-Geräten finden Sie unter "Zugriff auf remote Linux-Geräte [Webkonsole]" auf Seite 961.

Konfigurieren der Windows 2003-Clientsicherheit für die Remotesteuerung

Der residente Dienst verwendet die Windows NT-Sicherheit. Damit Sie mit Windows 2003-Server arbeiten können, müssen Sie die Serverclients so konfigurieren, dass das Windows 2003-Freigabe- und Sicherheitsmodell für lokale Konten "klassisch" konfiguriert ist (lokale Benutzer authentifizieren sich als sie selbst). Wenn Sie dies nicht tun, arbeitet die Gast-Standardauthentifizierung nicht mit der Windows NT-Sicherheit der Remotesteuerung zusammen.

So setzen Sie das Windows 2003-Sicherheitsmodell auf "klassisch"

1. Klicken Sie am Windows 2003-Client auf **Start > Systemsteuerung**.
2. Klicken Sie im Applet **Verwaltung > Lokale Sicherheitsrichtlinie** auf **Sicherheitsoptionen> Netzwerkzugriff**: **Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten** und wählen Sie die Einstellung **Klassisch - lokale Benutzer authentifizieren sich als sie selbst**.

Zugriff auf remote Linux-Geräte [Webkonsole]

Um eine Remote-Verbindung zu einem Linux-Gerät herzustellen, muss mindestens der Standard Management Agent auf dem betreffenden Gerät bereitgestellt worden sein. Wenn Sie in einer beliebigen Geräteliste der Webkonsole ein Linux-Gerät auswählen, haben Sie bei der Remotesteuerung die Wahl zwischen **SSH** und **SFTP**.

HINWEIS: Wenn auf dem Gerät bis dato kein Agent bereitgestellt worden ist und Sie in der Webkonsole einen Befehl zur **Remotesteuerung** wählen, wird der Windows Remote Control Viewer geöffnet, da das Betriebssystem noch nicht bekannt ist. Der Viewer meldet dann, dass er keine Verbindung zum Gerät herstellen kann.

So greifen Sie auf ein remotes Linux-Gerät zu

1. Wählen Sie das Gerät in einer Geräteliste der Webkonsole aus.
2. Klicken Sie im Aktionsbereich auf die Registerkarte **Eigenschaften**.
3. Klicken Sie entweder auf die Schaltfläche **SSH** oder auf die Schaltfläche **SFTP**.

Wenn Sie SSH-Zugriff auswählen, wird ein Fenster mit einer SSH-Sitzung auf dem Remotegerät geöffnet. Sie müssen einen Benutzernamen und ein Kennwort eingeben, um auf das Gerät zugreifen zu können. Wenn Sie sich authentifiziert haben, wird eine sichere Shell-Sitzung auf dem Remotegerät geöffnet.

Wenn Sie SFTP-Zugriff auswählen, wird ein Fenster mit einer sicheren FTP-Anzeige des Remotegeräts geöffnet (basierend auf einer SSH-Verbindung). Sie müssen einen Benutzernamen und ein Kennwort eingeben, um auf das Gerät zugreifen zu können. Nachdem Sie sich authentifiziert haben, können Sie mithilfe der sicheren FTP-Funktion Dateien von Ihrem Computer auf das Remotegerät (und umgekehrt) übertragen.

Planen von Tasks [Webkonsole]

Das Extra **Geplante Tasks** listet Verteilungstasks auf, die Sie von der LANDesk Management Console und von der Webkonsole aus ausgeführt haben. Die Tasks können mit der Agentenkonfiguration, mit Patch Manager, mit der Softwareverteilung, mit der Bereitstellung, mit Skripten und mit der Geräteerkennung in Zusammenhang stehen.

In der Webkonsole können Sie Pakete und Skripte, LaunchPad-Tasks, Richtlinien und Alarmregelsätze planen. Die Tasks werden im Aktionsbereich der jeweiligen Funktion angezeigt. Wenn Sie beispielsweise das Extra **Verteilung** öffnen, wird im Aktionsbereich eine Registerkarte **Geplante Tasks** angezeigt, auf der Ihre Paketverteilungstasks aufgeführt sind. Tasks für sämtliche dieser Extras sind ferner im Extrafenster **Geplante Tasks** aufgelistet.

HINWEIS: Sie können zwar Inventarscans sowie Patch- und Compliancescans vom Extra **Eigene Geräte** aus ausführen, aber diese Tasks werden nicht im Extra **Geplante Tasks** aufgelistet. Statusmeldungen für diese Scans werden nur im Aktionsbereich angezeigt.

Das Extrafenster **Geplante Tasks** zeigt folgende Taskgruppen:

- **Eigene Tasks:** Tasks, für die Sie einen Zeitplan erstellt haben. Nur Sie selbst und administrative Benutzer können diese Tasks sehen.

- **Öffentliche Tasks:** Tasks, die von Benutzern als "öffentlich" gekennzeichnet wurden. Jeder Benutzer, der von dieser Gruppe aus einen Task bearbeitet oder plant, wird Eigentümer dieses Tasks. Der Task verbleibt in der Gruppe "Öffentliche Tasks" und wird auch in der Gruppe "Benutzertasks" für diesen Benutzer angezeigt.
- **Alle Tasks:** Sowohl eigene als auch öffentliche Tasks.
- Alle Richtlinien:
- **Benutzertasks:** (Nur Benutzer mit Administratorrechten) Listet alle Tasks nach Eigentümer/Ersteller sortiert auf (ausschließlich öffentlicher Tasks).

Wenn Sie auf **Eigene Tasks**, **Öffentliche Tasks** oder **Alle Tasks** klicken, werden in der Taskliste folgende Informationen angezeigt:

- **Task:** Die Tasknamen.
- **Starten:** Zeitpunkt, zu dem die Ausführung des Task geplant ist. Klicken Sie auf einen Tasknamen und klicken Sie auf **Bearbeiten**, um die Uhrzeit für den Start zu bearbeiten.
- **Status:** Der allgemeine Taskstatus, also "In Arbeit", "Alle Vorgänge abgeschlossen", "Kein Vorgang abgeschlossen", "Nicht geplant", "Für Download verfügbar" oder "Fehlgeschlagen".
- **Verteilungspaket:** Der Name des Pakets, das der Task verteilt. Dieses Feld gilt nur für Verteilungspakete.
- **Verteilungsmethode:** Die vom Task verwendete Verteilungsmethode. Dieses Feld gilt nur für Verteilungspakete.
- **Eigentümer:** Der Name der Person, die den Task geplant hat.
- **Taskkennung**: Eine sequenzielle Zahl, die Tasks in der Datenbank zugeordnet wird.

Wenn Sie auf einen geplanten Task doppelklicken, werden im Extrabereich folgende Informationen angezeigt:

- **Name:** Der Name des Taskstatus.
- **Menge:** Die Geräteanzahl pro Taskstatus.
- **Prozentsatz:** Der Prozentsatz an Geräten in jedem Taskstatus.

Damit Sie einen geplanten Task für ein Gerät konfigurieren können, muss das Gerät über den entsprechenden Agenten verfügen und in der Inventardatenbank registriert sein. Serverkonfigurationen bilden eine Ausnahme. Sie können ein Gerät als Ziel auswählen, auf dem nicht der Standard Management Agent installiert ist.

Tasks können entweder im Extra "Geplante Tasks" bzw. dem Aktionsbereich für das spezifische Extra neu geplant, bearbeitet oder gelöscht werden. Um einen Task zu bearbeiten, wählen Sie ihn aus und klicken auf die Schaltfläche **Bearbeiten** in der Symbolleiste.

Erstellen von benutzerdefinierten Taskgruppen

Sie können benutzerdefinierte Gruppen für die Tasktypen **Eigene Tasks** und **Öffentliche Tasks** erstellen. Mithilfe benutzerdefinierter Gruppen können Sie verwandte Tasks, z. B. das Scannen nach Anfälligkeiten und Ausführen eines Skripts, zu Gruppen zusammenfassen.

So erstellen Sie eine benutzerdefinierte Taskgruppe

1. Klicken Sie in der Toolbox der Webkonsole auf **Verteilung > Geplante Tasks**.
2. Wählen Sie die Taskgruppe aus, in der Sie eine benutzerdefinierte Gruppe erstellen möchten.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue Gruppe**.
4. Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **OK**.
5. Um Tasks oder andere Gruppen in die Gruppe zu verschieben, wählen Sie diese aus einer Liste aus und klicken in der Symbolleiste auf die Schaltfläche **Verschieben**. Wählen Sie Ihre benutzerdefinierte Gruppe aus und klicken Sie auf **OK**.

Verschieben von Tasks

Verwenden Sie die Symbolleistenschaltfläche **Verschieben**, um einen Task aus einer Taskgruppe in eine andere Gruppe zu verschieben und somit den Task für Benutzer sichtbar zu machen, die befugt sind, die Taskgruppe anzuzeigen, in die Sie den Task verschieben.

1. Wählen Sie im Extra **Geplante Tasks** oder auf der Registerkarte **Tasks** eines Webkonsolenextras einen Task aus einer der Gruppen ("Eigene Tasks", "Öffentliche Tasks", "Alle Tasks oder Benutzertasks).
2. Klicken Sie auf die Schaltfläche **Verschieben** in der Symbolleiste.
3. Wählen Sie die Taskgruppe aus, in die Sie den Task verschieben möchten, und klicken Sie dann auf **OK**.

Hilfe zum Task Scheduler

Die folgenden Abschnitte beschreiben Optionen in Dialogfeldern, die im Zusammenhang mit der Taskplanung in der Webkonsole stehen.

- Die Seite "Übersicht"
- Die Seite "Benutzerdefinierte Skripte"
- Die Seite "Zielgeräte"
- Die Seite "Task planen"
- Die Seite "Verteilungspaket"
- Die Seite "Verteilungsmethoden"
- Die Seite "Anmeldeinformationen"
- Die Seite "Abbildinformationen"
- Die Seite "Zusätzliche Befehle"
- Die Seite "LANDesk Agent"
- Die Seite "DOS-Befehle"

Informationen zur Seite "Übersicht"

- Eigentümer: gibt den aktuellen Eigentümer des Tasks an. Sie können einen anderen Benutzer als Eigentümer auswählen oder "Öffentlich" oder "Öffentlicher Benutzer" wählen, um den Task in der Gruppe "Öffentliche Tasks" zu speichern.
- **Aktuell ausgewähltes Element**: zeigt den Namen des Elements an, das derzeit geplant wird. Klicken Sie auf **Ändern**, um die Seite zum manuellen Festlegen aufzurufen und ein anderes Element auszuwählen.

- Zurzeit ausgewählte Ziele: zeigt die Geräte an, die als Ziele für den Task festgelegt wurden. Klicken Sie auf **Ändern**, um die Seite **Zielgeräte** aufzurufen und die Ziele zu ändern.
- **Geplante Zeit:** zeigt an, wann der Task geplant ist. Klicken Sie auf **Ändern**, um die Seite **Task planen** aufzurufen und die Zeit zu ändern.

Informationen zur Seite "Benutzerdefinierte Skripte"

- **Zurzeit ausgewähltes benutzerdefiniertes Skript:** Klicken Sie auf das Skript, für das Sie eine Planung durchführen möchten.

Informationen zur Seite "Zielgeräte"

Verwenden Sie diese Seite, um Geräteziele für den von Ihnen konfigurierten Task hinzuzufügen. Auf dieser Registerkarte können Sie auch die Zielgeräte, Abfragen und Gerätegruppen für den Task anzeigen.

Drei Dropdownlisten enthalten Abfragen, LDAP-Abfragen und Gruppen, die Sie in der Netzwerkansicht von Management Suite erstellt haben.

- **Zielliste hinzufügen:** Fügt die Geräte hinzu, die aus der Liste **Eigene Geräte** zur Zielliste hinzugefügt wurden. (Eine Anweisung finden Sie unter Zielgeräte definieren.)
- **LDAP-Liste hinzufügen:** Wählen Sie ein LDAP-Objekt aus, das Sie aus der **Verzeichnis-Manager**-Struktur zur Zielliste hinzugefügt haben.
- **Abfrage hinzufügen:** Wählen Sie eine Abfrage aus der ersten Liste aus und klicken Sie auf diese Schaltfläche, um die Ergebnisse der Abfrage zur Zielliste hinzuzufügen.
- **LDAP-Abfrage hinzufügen:** Wählen Sie eine LDAP-Abfrage aus der zweiten Liste aus und klicken Sie auf diese Schaltfläche, um die Ergebnisse einer LDAP-Abfrage zur Zielliste hinzuzufügen.
- **Gruppe hinzufügen:** Wählen Sie eine Gruppe aus der dritten Liste aus und klicken Sie auf diese Schaltfläche, um den Inhalt der Gruppe zur Zielliste hinzuzufügen.
- **Geräte reaktivieren:** Markieren Sie dieses Kontrollkästchen, wenn die Zielgeräte (die heruntergefahren wurden oder sich im Ruhe- oder Energiesparmodus befinden) beim Starten des Tasks reaktiviert werden sollen.
- **Entfernen:** Wählen Sie ein Zielelement aus und klicken Sie auf diese Schaltfläche, um diese Zielgeräte zu entfernen.

HINWEIS: In der Webkonsole werden Gerätegruppen nicht in Form einer Gruppe als Ziel angesprochen. Vielmehr werden die einzelne Geräte in der Gruppe zur Liste der Zielgeräte hinzugefügt, wenn Sie eine Gruppe auswählen und als Ziel definieren.

Informationen zur Seite "Task planen"

- **Ungeplant lassen**: (Standard) Bewahrt den Task für künftige Zeitpläne in der Taskliste auf.
- **Jetzt starten**: Führt den Task so bald wie möglich aus. Je nach Einstellung kann es bis zu einer Minute dauern, bevor der Task gestartet wird.
- **Zum geplanten Zeitpunkt starten**: Startet den Task zu der von Ihnen angegebenen Uhrzeit. Geben Sie die folgenden Optionen an:
  - **Datum**: Das Datum für den Beginn des Tasks.
  - **Uhrzeit**: Die Uhrzeit für den Taskbeginn.

- **Wiederholen jede(n):** Wenn Sie den Task wiederholt ausführen möchten, wählen Sie den Zeitraum aus (jede Stunde, jeden Tag, jede Woche oder jeden Monat). Wenn Sie **Monat** auswählen und das Datum nicht in allen Monaten existiert (beispielsweise der 31.), wird der Task nur in den Monaten ausgeführt, in denen das Datum existiert.

- **Diese Geräte planen:** Behalten Sie beim ersten Ausführen eines Tasks den Standardwert **Alle** bei. Für nachfolgende Läufe wählen Sie eine der folgenden Optionen:
  - **Fehlgeschlagene Geräte:** Wählen Sie diese Option aus, wenn der Task nur auf den Geräten ausgeführt werden soll, auf denen der Task beim ersten Durchlauf nicht ausgeführt werden konnte. Dies schließt Geräte mit dem Status "Erfolgreich" aus. Der Task wird auf Geräten mit anderen Zuständen ausgeführt, beispielsweise "Wartemodus" oder "Aktiv". Ziehen Sie die Verwendung dieser Option in Betracht, wenn Sie den Task auf so vielen Geräten wie möglich ausführen möchten, auf denen die Ausführung misslungen ist, der Task jedoch nur einmal pro Gerät erfolgreich ausgeführt werden muss.
  - **Im Wartezustand oder zurzeit aktiv:** Wählen Sie diese Option aus, wenn Sie den Task auf Geräten ausführen möchten, die sich in der Verarbeitungswarteschlange befinden oder der Verarbeitung zurzeit läuft.
  - **Alle:** Wählen Sie diese Option aus, wenn Sie den Task, unabhängig vom Zustand, auf allen Geräten ausführen möchten. Ziehen Sie die Verwendung dieser Option in Betracht, wenn es sich um einen Task (insbesondere einen wiederholt auszuführenden Task) handelt, der auf so vielen Geräten wie möglich ausgeführt werden muss.
  - **Geräte, die nicht versucht haben, den Task auszuführen:** Wählen Sie diese Option, wenn der Task nur auf Geräten ausgeführt werden soll, die den Task nicht vollständig ausgeführt haben, auf denen die Taskausführung aber nicht fehlgeschlagen ist. Dies schließt Geräte aus, deren Zustand "Aus", "Beschäftigt", "Fehlgeschlagen" oder "Abgebrochen" war. Ziehen Sie die Verwendung dieser Option in Betracht, wenn es zahlreiche Zielgeräte gab, auf denen der Task fehlschlug, diese Geräte als Ziele jedoch nicht wichtig sind.

Informationen zur Seite "Verteilungspaket"

(Nur Verteilungspakete) Das Hauptpaket ist standardmäßig ausgewählt. Sie können das Hauptpaket ändern, indem Sie es auswählen und auf die Schaltfläche **Entfernen** klicken. Sie können ein anderes Paket vor oder nach dem Hauptpaket ausführen, indem Sie **Vorläufiges Paket** oder **Letztes Paket** wählen und dann ein Paket aus der Liste auswählen.

- **Typ:** Der Typ des auszuführende Pakets. Wählen Sie einen Pakettyp in der Liste aus, um die verfügbaren Pakete dieses Typs im nachstehenden Feld anzuzeigen.
- **Vorläufiges Paket:** Diese Option wählen Sie, wenn Sie bei einer Mehrpaketverteilung ein weiteres Paket vor dem Hauptpaket hinzufügen möchten. Wählen Sie einen Pakettyp aus, suchen Sie das Paket und klicken Sie auf **Festlegen**, um es zur Mehrpaketverteilung hinzuzufügen.
- **Hauptpaket:** Das wichtigste auszuführende Paket. Wenn Sie das Hauptpaket ändern möchten, wählen Sie diese Option, wählen Sie einen Pakettyp aus und suchen Sie das Paket. Klicken Sie auf **Festlegen**, um dieses Paket als Hauptpaket zu definieren.
- **Letztes Paket:** Diese Option wählen Sie, wenn Sie bei einer Mehrpaketverteilung ein weiteres Paket nach dem Hauptpaket hinzufügen möchten. Wählen Sie einen Pakettyp aus, suchen Sie das Paket und klicken Sie auf **Festlegen**, um es zur Mehrpaketverteilung hinzuzufügen.
- **Festlegen:** Klicken Sie auf diese Schaltfläche, um die ausgewählte Paketoption zur Spalte "Reihenfolge" hinzuzufügen.

- **Reihenfolge:** Die Reihenfolge, in der Pakete auszuführen sind. Die Reihenfolge ist "Vorläufiges Paket", "Hauptpaket" und "Letztes Paket".
- **Entfernen:** Entfernt das ausgewählte Paket aus der Spalte "Reihenfolge".

Informationen zur Seite "Verteilungsmethode"

(Nur Verteilungspakete) Die Verteilungsmethode bestimmt, wie das Paket an die Geräte gesendet wird.

- **Typ:** Wählen Sie hier zunächst den Typ der Verteilungsmethode (Richtlinienunterstütztes Push, Push, Richtlinie oder Multicast) und dann eine spezifische Methode aus dieser Gruppe.
- **Verteilungsmethode:** Wählen Sie eine der Verteilungsmethoden aus, die Sie in der LANDesk Management Console oder in der Webkonsole erstellt haben.

Informationen zur Seite "Anmeldeinformationen"

- **Benutzername:** Identifiziert ein Benutzerkonto, das über die Anmeldeinformationen verfügt, die für die Anmeldung bei der Netzwerkfreigabe erforderlich sind.
- **Kennwort:** Stellt das Kennwort des Benutzers bereit.
- **Domäne:** Active Directory-Domäne des Benutzers.

Informationen zur Seite "Abbildinformationen"

Auf dieser Seite geben Sie an, welcher Abbildtyp mit diesem Skript wiederhergestellt werden soll, wo das Abbild gespeichert wird und in welchem Verzeichnis sich das Abbilderstellungstool befindet.

- **Abbildtyp:** Bezeichnung des Dateityps (Formats) der vorhandenen Abbilddatei, die mit diesem Skript bereitgestellt werden soll; der Dateityp wird durch die Auswahl eines Tools aus der Liste der Abbildverarbeitungstools festgelegt.
- **UNC-Pfad zur wiederherzustellenden Abbilddatei:** Gibt den Server und die Freigabe an, die als Speicherort für die Abbilddatei dienen, einschließlich des Dateinamens des Abbilds. Das Abbild muss in einem für Geräte zugänglichen freigegebenen Ordner gespeichert werden.
- **UNC-Pfad zum Abbildverarbeitungstool:** Gibt den Server und die Freigabe an, die als Speicherort für das Abbildverarbeitungstools (das dem oben ausgewählten Abbildtyp entspricht) dienen, einschließlich des Namens der ausführbaren Datei des Tools.

Informationen zur Seite "Zusätzliche Befehle"

- **Geben Sie Befehle ein, die vor dem Neustart und vor der Abbilderstellung des Geräts ausgeführt werden sollen:** Geben Sie Befehle ein, die vor dem Neustart und vor der Abbilderstellung des Geräts auszuführen sind.
- **Zusätzliche Befehlszeilenparameter für das Abbildverarbeitungstool eingeben:** Geben Sie zusätzliche Parameter ein, die zuvor nicht angegeben wurden.

Informationen zur Seite "LANDesk Agent"

- **UNC-Pfad:** Der Pfad zum Agentenpaket.
- **Benutzername:** Identifiziert ein Benutzerkonto, das über die Anmeldeinformationen verfügt, die für die Anmeldung bei der Netzwerkfreigabe erforderlich sind.
- **Kennwort:** Stellt das Kennwort des Benutzers bereit.
- **Domäne:** Active Directory-Domäne des Benutzers.

Informationen zur Seite "DOS-Befehle"

- **DOS-Befehle:** Geben Sie DOS-Befehle ein, die zum Zeitpunkt der Bereitstellung auf dem Gerät ausgeführt werden sollen.
- **Diesen Auftrag abbrechen, wenn ein Befehl fehlschlägt:** Stoppt den Task, falls ein Befehl fehlschlägt, und stellt den vorherigen Zustand des Geräts wieder her.

Anzeigen des Alarmprotokolls [Webkonsole]

Verwenden Sie die Seite **Alarmprotokoll** zum Anzeigen von Alarmen, die an den Coreserver gesendet wurden. Das Protokoll wird nach der Uhrzeit (GMT) sortiert, wobei sich der jüngste Alarm am Anfang des Protokolls befindet.

So zeigen Sie das globale Alarmprotokoll an

1. Klicken Sie in der Toolbox der Webkonsole auf **Überwachung > Alarmprotokoll**.
2. Klicken Sie auf eine Spaltenüberschrift, um Einträge anhand der Spalte zu sortieren.
3. Doppelklicken Sie auf den Eintrag in der Spalte **Alarmname**, um eine ausführliche Beschreibung eines Alarms anzuzeigen.
4. Um die Protokolleinträge nach Alarmname, Status, Instanz, Gerätename oder IP-Adresse aufzulisten, wählen Sie die entsprechenden Kriterien in der Liste **Filter** aus. Wählen Sie beispielsweise **Alarmname** aus und geben Sie einen vollständigen Namen ein (z. B."Leistung"); oder geben Sie mit dem Platzhalter * einen Teil eines Namens in das Filtertextfeld ein (z. B. "Remote*"). Um einen Suchvorgang nach dem Datum auszuführen, wählen Sie **Datumsfilter aktivieren** aus und geben ein Anfangsdatum und ein Enddatum ein. Wenn Sie Filterkriterien hinzugefügt haben, klicken Sie in der Symbolleiste auf **Suchen**.
5. Um den Zustandsstatus eines Alarms zu löschen, wählen Sie in der Spalte **Alarmname** den Alarm aus, klicken in der Symbolleiste auf die Schaltfläche **Bestätigen** und dann auf **OK**.
6. Um einen Protokolleintrag zu löschen, klicken Sie mit der rechten Maustaste auf den Alarm und wählen **Eintrag löschen**.
7. Um alle Einträge im Protokoll zu löschen, klicken Sie mit der rechten Maustaste auf eine Zeile in der Spalte **Alarmname** und wählen **Protokoll löschen** aus.

HINWEIS: Wenn der Gerätename nicht als vollständig qualifizierter Domänenname angezeigt wird, so liegt das daran, dass das Produkt nicht in der Lage war, den vollständig qualifizierten Domänennamen für das Gerät aufzulösen.

Klicken Sie hier, um Beschreibungen der verschiedenen Spalten des Alarmprotokolls anzuzeigen.

- **Alarmname:** Der mit dem Alarm assoziierte Name - wie auf der Seite **Alarmkonfigurationen** definiert.
- **Zeit:** Das Datum und die Uhrzeit, zu der der Alarm generiert wurde (GMT).
- **Status:** Der Schweregrad des Alarms, wobei folgende Statusangaben unterstützt werden:
  - **Unbekannt:** Der Status lässt sich nicht ermitteln.
  - **Zur Information:** Unterstützt Konfigurationsänderungen oder Ereignisse, die Hersteller u. U. in ihre Systeme einschließen.
  - **OK:** Gibt an, dass der Status sich auf einem akzeptablen Niveau befindet.

  - **Warnung:** Macht auf ein sich abzeichnendes Problem aufmerksam, bevor ein kritischer Punkt erreicht wird.
  - **Kritisch:** Gibt an, dass dem Problem sofortige Aufmerksamkeit geschenkt werden muss.
- **Instanz:** Liefert detaillierte Informationen zu der Situation, in der der Alarm generiert wurde.
- **Gerätename:** Der Name des Geräts, auf dem der Alarm generiert wurde. Dies sollte ein vollständig qualifizierter Domänenname sein.
- **IP-Adresse:** Die IP-Adresse des Geräts, auf dem der Alarm generiert wurde.

Verwenden von Abfragen [Webkonsole]

Abfragen sind benutzerdefinierte Suchvorgänge, die in den Core-Datenbanken ausgeführt werden. Mithilfe von Abfragen können Sie auf der Basis bestimmter System- oder Benutzerkriterien nach in der Coredatenbank gespeicherten Geräten suchen und diese entsprechend ordnen. Damit steht Ihnen ein praktisches Hilfsmittel für die Netzwerkverwaltung zur Verfügung.

So können Sie beispielsweise eine Abfrage erstellen und ausführen, die nur Geräte mit einer Taktgeschwindigkeit von weniger als 2 GHz, weniger als 4 GB Arbeitsspeicher oder einer Festplatte mit weniger als 80 GB Speicherkapazität zurückgibt. Erstellen Sie eine oder mehrere Abfrageanweisungen für diese Bedingungen und verknüpfen Sie diese Anweisungen mithilfe von logischen Operatoren. Wenn die Abfragen ausgeführt wurden, können Sie die Ergebnisse drucken, auf die entsprechenden Geräte zugreifen und sie verwalten.

Sie können in Management Suite Datenbankabfragen für Geräte in Ihrer Coredatenbank erstellen und Sie können LDAP-Abfragen für Geräte erstellen, die sich in anderen Verzeichnissen befinden.

In der Webkonsole können Sie mit dem Extra **Abfragen** Coredatenbankabfragen erstellen. LDAP-Abfragen werden mit dem Tool **Verzeichnis-Manager** erstellt.

Anzeigen der verfügbaren Abfragen

Die Seite **Benutzerdefinierte Abfragen** zeigt eine Liste mit Abfragen an, die von Ihnen entweder in der Netzwerkansicht von Management Suite oder in der Webkonsole erstellt wurden.

So zeigen Sie die verfügbaren Abfragen an

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Abfragen**.
2. Erweitern Sie die Gruppen (Meine Abfragen, Öffentliche Abfragen oder Alle Abfragen), um eine Abfrage zu finden.
3. Klicken Sie mit der rechten Maustaste auf eine Abfrage, um sie zu bearbeiten, zu löschen oder auszuführen.

Ausführen von Abfragen in der Webkonsole

So führen Sie eine Abfrage aus

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Abfragen**.
2. Erweitern Sie die Gruppen (Meine Abfragen, Öffentliche Abfragen oder Alle Abfragen), um eine Abfrage zu finden.
3. Wählen Sie die Abfrage aus und klicken Sie in der Symbolleiste auf die Schaltfläche **Ausführen**.

   Die Abfrageergebnisse werden im Extrabereich angezeigt.

4. Um die Abfrageergebnisse zu drucken, klicken Sie in der Symbolleiste auf die Schaltfläche **Druckvorschau**. Die vollständigen Abfrageergebnisse werden in einem Tabellenformat aufgelistet. Sie können die Liste mit der Druckfunktion Ihres Browsers ausdrucken.
5. Um die Abfrageergebnisse in einer CSV-Datei zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Als CSV speichern** und geben den Speicherort für die Datei an.
6. Um eine kurze Inventarzusammenfassung für ein Gerät in den Abfrageergebnissen anzuzeigen, klicken Sie mit der rechten Maustaste auf das Gerät und anschließend auf **Computer anzeigen**.

HINWEIS: Wenn sich das Abfrageergebnis über mehrere Seiten erstreckt, können Sie mit den Pfeilen oben rechts auf der Seite zwischen den Seiten hin- und herblättern. Geben Sie an, wie viele Elemente pro Seite angezeigt werden sollen, und klicken Sie auf **Festlegen**.

Erstellen von benutzerdefinierten Abfragen [Webkonsole]

Benutzerdefinierte Abfragen sind nützlich, wenn Sie Inventardetails zu Hardware- und Softwareprodukten, die auf Ihren Geräten installiert sind, abrufen möchten. Verwenden Sie eine benutzerdefinierte Abfrage dazu, Geräte, die über ein ähnliches Inventar verfügen, in einer Liste zusammenzufassen. Wenn Sie beispielsweise Geräte auf einen Prozessor mit 2 GHz aufrüsten möchten, können Sie alle Geräte mit einer Prozessorgeschwindigkeit unter 2 GHz aus der Datenbank extrahieren. Benutzerdefinierte Abfragen werden auch zum Definieren von Gruppen und Bereichen verwendet.

Sie können alle Inventarelemente ("Attribute" genannt) abfragen, die der Inventarscanner in der Datenbank speichert.

Verwalten von Abfragen

Abfragen verwalten Sie im Extrabereich **Abfragen**. Dieses Extra verwenden Sie zum Erstellen, Bearbeiten oder Löschen von Abfragen:

- Um eine vorhandene Abfrage auszuführen, wählen Sie sie aus und klicken auf **Ausführen**.
- Um eine neue Abfrage zu erstellen, klicken Sie auf **Neu**. Sobald Sie die Abfrage erstellt und gespeichert haben, wird der Name in der Liste auf dieser Seite angezeigt.
- Zum Bearbeiten einer Abfrage in der Liste doppelklicken Sie auf die Abfrage. Die Seite **Abfrage bearbeiten** wird angezeigt. Sie enthält Abfrageparameter, die von Ihnen bearbeitet werden können.
- Zum Bearbeiten der letzten Abfrage klicken Sie auf **Aktuelle Abfrage bearbeiten**.
- Um eine Abfrage zu entfernen, wählen Sie die Abfrage aus und klicken auf **Löschen**.
- Um die Abfrageparameter auf der Seite **Abfrage bearbeiten** zu entfernen, klicken Sie auf die Symbolleistenschaltfläche **Löschen**. Wurde die Abfrage bereits gespeichert, wird sie auf dieser Seite entfernt, bleibt aber in der Liste **Benutzerdefinierte Abfragen** gespeichert.

Zum Erstellen einer Abfrage sind vier Schritte erforderlich:

1. **Eine Suchbedingung erstellen:** Geben Sie eine Reihe von Inventarattributen an, die die Grundlage der Abfrage bilden.
2. **Attribute zum Anzeigen auswählen:** Optimieren oder "filtern" Sie die Abfrage so, dass die Ergebnisse die für Sie nützlichsten Attribute anzeigen, wie z. B. IP-Adressen oder Gerätenamen.

3. **Sortieren der Ergebnisse nach Attributen:** Geben Sie an, wie die Abfrageergebnisse sortiert werden sollen. (Diese Optionen kommen nur dann zur Anwendung, wenn Sie in Schritt 2 mehr als einen Attributtyp zur Anzeige in den Abfrageergebnissen ausgewählt haben.)
4. **Abfrage ausführen:** Führen Sie die soeben erstellte Abfrage aus. Sie können sie auch zur späteren Verwendung speichern oder alle Abfragedaten löschen und eine neue Abfrage erstellen.

Schritt 1: Erstellen einer Verteilungsmethode [Webkonsole]

Eine Suchbedingung besteht aus einer Reihe von Inventarattributen und verknüpften Werten, die von Ihnen abgefragt werden. Als Grundlage für eine Abfrage können Sie eine einzelne Suchbedingung verwenden oder mehrere Suchbedingungen zu einer Gruppe zusammenstellen.

Die folgenden Schritte führen Sie auf der Seite **Abfrage bearbeiten** aus. Klicken Sie in der Ansicht **Benutzerdefinierte Abfragen** auf **Neu** oder wählen Sie eine vorhandene Abfrage und klicken Sie auf **Bearbeiten**.

So erstellen Sie eine Suchbedingung

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Abfragen**.
2. Klicken Sie in der Symbolleiste auf **Neu** oder wählen Sie eine vorhandene Abfrage aus und klicken Sie auf **Bearbeiten**.
3. Klicken Sie unter **Schritt 1** auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
4. Wählen Sie die Attribute in der Liste aus, die Sie als Suchbedingung festlegen möchten. Um beispielsweise alle Clients zu suchen, die eine bestimmte Software ausführen, wählen Sie Computer.Software.Paket.Name.
5. Nach dem Auswählen der Attribute wird auf der rechten Seite des Fensters eine Reihe von Feldern angezeigt. Wählen Sie aus diesen Feldern einen Operator und Wert aus, um die Suchbedingung zu vervollständigen. Um beispielsweise alle Clients zu finden, die Internet Explorer 7.0 ausführen, wählen Sie die Attribute "Computer.Software.Paket.Name", den Operator "=" und den Wert "Internet Explorer". Wählen Sie den Booleschen Operator AND aus und klicken Sie auf **Hinzufügen**. Wählen Sie die Attribute "Computer.Software.Paket.Name", den Operator "LIKE" und den Wert "8" und klicken Sie auf **Hinzufügen**.
6. Sie können die Abfrage weiter verfeinern, indem Sie eine weitere Suchbedingung erstellen und sie der ersten Bedingung mit einem Booleschen Operator (AND oder OR) hinzufügen. Über die Schaltflächen können Sie Bedingungen hinzufügen, löschen, ersetzen, gruppieren oder die Gruppierung aufheben.
7. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

HINWEIS: Bevor Sie eine Abfrage zum Zustand eines Servers (Computer.Zustandsstatus) ausführen und speichern, sollten Sie berücksichtigen, dass der Zustand des Servers in der Datenbank durch eine Nummer repräsentiert wird. Verwenden Sie die Tabelle weiter unten, um Suchbedingungen zu erstellen. Um z. B. eine Suchbedingung für Rechner mit dem Zustand "Unbekannt" zu erstellen, verwenden Sie den Operator "NOT EXISTS".

Zustand	Operator
Unbekannt	NOT EXISTS

Zustand	Operator
Normal	2
Warnung	3
Kritisch	4

Schritt 2: Auswählen der anzuzeigenden Attribute [Webkonsole]

In Schritt 2 wählen Sie Attribute aus, die besonders nützlich sind, um die in den Abfrageergebnissen zurückgegebenen Computer zu identifizieren. Wenn Sie anhand der Ergebnisse beispielsweise jeden Computer, der den in Schritt 1 angegebenen Suchbedingung entspricht, physikalisch orten möchten, geben Sie Attribute wie den Anzeigenamen des Computers (Computer.Anzeigename) oder die IP-Adresse (Computer.Netzwerk.TCPIP.Adresse) an.

So wählen Sie Attribute zum Anzeigen aus

1. Klicken Sie auf der Seite **Abfrage bearbeiten** unter **Schritt 2** auf **Bearbeiten**. Es wird ein Fenster mit einer Liste angezeigt, die alle momentan in der Datenbank vorhandenen Inventardaten enthält.
2. Führen Sie einen Drilldown auf dieser Liste durch, um ein Attribut auszuwählen, das in der Abfrageergebnisliste angezeigt werden soll. Wählen Sie dabei Attribute aus, mit denen Sie die in der Abfrage zurückgegebenen Clients identifizieren können.

   HINWEIS: Wenn Sie eine Oracle-Datenbank verwenden, wählen Sie mindestens ein Attribut aus, das direkt durch den Inventarscanner definiert ist (z. B. Computer.Anzeigename, Computer.Gerätename, Computer.Gerätekennung, Computer.Anmeldename usw.).

3. Klicken Sie auf **Hinzufügen**, nachdem Sie ein Attribut ausgewählt haben, um es in das Feld in der unteren Hälfte des Fensters zu verschieben.
4. Wenn Sie die Abfrageergebnisse in der Liste auflisten möchten, wählen Sie **Anzahl aufnehmen**.
5. Wiederholen Sie den Vorgang, um weitere Attribute hinzuzufügen. Verwenden Sie die Pfeiltasten, um Attribute hinzuzufügen oder zu entfernen. Klicken Sie auf **Nach oben** oder **Nach unten**, um die Reihenfolge der Attribute zu ändern.
6. Um die Ergebnisse der Abfrage als Ziel für jede von Ihnen angegebene Aktion auswählbar zu machen, klicken Sie auf **Ergebnisse als Ziel auswählbar machen**.
7. Wenn Sie alle Attribute ausgewählt haben, klicken Sie auf **OK**.

Sie können die Spaltenüberschriften in Ihrer Abfrageergebnisliste auch bearbeiten.

So ändern Sie Spaltenüberschriften

1. Klicken Sie unter **Schritt 2** auf **Bearbeiten**.
2. Klicken Sie im unteren Feld auf eine Spaltenüberschrift und klicken Sie dann auf **Bearbeiten**. Bearbeiten Sie die Überschrift und drücken Sie die **Eingabetaste**. Wiederholen Sie diesen Schritt nach Bedarf.
3. Klicken Sie auf **OK**.

An diesem Punkt sollten Sie Ihre Abfrage speichern. Das sich anschließende Verfahren zur Abfrageerstellung ist optional und nur für Abfrageergebnisse anwendbar, die zwei oder mehr Spalten aufweisen. Um Ihre Abfrage zu speichern, klicken Sie in der Symbolleiste auf die Schaltfläche **Speichern**. Geben Sie einen Namen in das Dialogfeld **Abfrage speichern** ein, wählen Sie eine Gruppe aus und klicken Sie auf **Speichern**.

Schritt 3: Sortieren der Ergebnisse nach Attribut [Webkonsole]

Dieser Schritt muss nur ausgeführt werden, wenn Sie in Schritt 2 mehr als ein Attribut oder eine Spaltenüberschrift definiert haben und die Ergebnisse alphabetisch oder numerisch innerhalb einer Spalte sortieren möchten.

Wenn Sie beispielsweise zwei verschiedene Attribute zur Anzeige der Abfrageergebnisse (die IP-Adresse und den Prozessortyp) angegeben haben, könnten Sie in den Ergebnisse alphabetisch nach Prozessortyp sortieren.

Wenn Sie diesen Schritt überspringen, wird die Abfrage automatisch nach dem ersten, in Schritt 2 gewählten Attribut sortiert.

So sortieren Sie die Ergebnisse nach Attribut

1. Klicken Sie auf der Seite **Abfrage bearbeiten** unter **Schritt 3** auf **Bearbeiten**. Es wird ein Fenster geöffnet, in dem die von Ihnen in **Schritt 2** ausgewählten Attribute angezeigt werden.
2. Wählen Sie das Attribut, nach dem sortiert werden soll, und klicken Sie anschließend auf **>>**, um es in das Feld **Ausgewählte Attribute** zu verschieben.
3. Klicken Sie auf **OK**.

Schritt 4: Ausführen der Abfrage [Webkonsole]

Nachdem Sie Ihre Abfrage erstellt haben, können Sie sie ausführen, speichern oder löschen, falls Sie noch einmal von vorne beginnen möchten.

So speichern Sie die Abfrage für eine zukünftige Verwendung

1. Klicken Sie auf der Seite **Abfrage bearbeiten** auf die Symbolleistenschaltfläche **Speichern**. Die Abfrage wird nun auf der Seite **Benutzerdefinierte Abfragen** aufgelistet.
2. Wenn es sich bei Ihrer Abfrage um eine geänderte Version einer vorhandenen Abfrage handelt, klicken Sie auf die Symbolleistenschaltfläche **Speichern unter**, um die Abfrage umzubenennen.

Standardmäßig sind gespeicherte Abfragen nur für den Benutzer sichtbar, der sie gespeichert hat. Wenn Sie vor dem Speichern das Kontrollkästchen **Öffentliche Abfrage** aktivieren, ist die Abfrage für alle Benutzer sichtbar. Nur Administratoren, die befugt sind, öffentliche Abfragen zu verwalten, können eine Abfrage öffentlich machen.

So zeigen Sie die Ergebnisse einer Abfrage an

- Klicken Sie in der Symbolleiste auf die Schaltfläche **Ausführen**.

HINWEIS: Die Anweisungen der Abfrage werden in der gezeigten Reihenfolge ausgeführt. Wenn keine Gruppierungen vorgenommen wurden, werden die Abfrageanweisungen von unten nach oben ausgeführt. Fassen Sie miteinander in Bezug stehende Elemente in Gruppen zusammen, sodass sie als Gruppe ausgewertet werden; andernfalls fallen die Ergebnisse Ihrer Abfrage eventuell anders als erwartet aus.

Anzeigen von Abfrageergebnissen [Webkonsole]

Das Ergebnis einer Abfrage entspricht den Suchkriterien, die Sie beim Definieren der Abfrage angegeben haben. Wenn das Ergebnis nicht Ihren Erwartungen entspricht, kehren Sie zur Seite **Abfrage bearbeiten** zurück und bearbeiten Sie die Informationen.

So zeigen Sie Inventarinformationen zu einem Gerät in den Abfrageergebnissen an

- Klicken Sie mit der rechten Maustaste auf den Gerätenamen und wählen Sie **Computer anzeigen**.

So zeigen Sie die Ergebnisse einer Abfrage an

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Druckvorschau**. Die vollständigen Abfrageergebnisse werden in einem Tabellenformat aufgelistet.
2. Drucken Sie die Liste mit der Funktion **Drucken** Ihres Browsers aus.

So speichern Sie Abfrageergebnisse in einer CSV-Datei

1. Klicken Sie in der Symbolleiste auf die Schaltfläche **Als CSV speichern**.
2. Geben Sie einen Speicherort für die Datei an.

Exportieren von Abfrageergebnissen in eine CSV-Datei [Webkonsole]

Um die Ergebnisdaten Ihrer Abfrage in einer Kalkulationstabelle oder einem anderen Programm anzuzeigen, exportieren Sie die Daten als Datei mit kommagetrennten Werten (CSV-Datei).

So speichern Sie Abfrageergebnisse in einer CSV-Datei

1. Klicken Sie auf der Seite **Abfrageergebnisse** auf die Symbolleistenschaltfläche **Als CSV speichern**.
2. Geben Sie einen Speicherort für die Datei an.

Exportieren und Importieren von Abfragen [Webkonsole]

Sie können jede von Ihnen erstellte Abfrage exportieren oder importieren. Alle Abfragen werden als XML-Dateien exportiert.

Die Funktionen zum Exportieren und Importieren sind in zwei Szenarien nützlich:

- Wenn Sie Ihre Datenbank erneut installieren müssen, verwenden Sie die Export- und Importfunktionen, um Ihre vorhandenen Abfragen für die Verwendung in einer neuen Datenbank zu speichern.

  Sie können die Abfragen beispielsweise exportieren und in ein Verzeichnis verschieben, das von einer Neuinstallation der Datenbank nicht betroffen ist. Nachdem Sie die Datenbank neu installiert haben, können Sie die Abfragen wieder in das Abfrageverzeichnis auf Ihrem Webserver verschieben und anschließend in die neue Datenbank importieren.

- Sie können die Export-/Importfunktionen verwenden, um Abfragen in andere Datenbanken zu kopieren.

  Sie können beispielsweise eine Abfrage in ein Abfrageverzeichnis auf dem Webserver exportieren und sie dann an einen anderen LANDesk Administrator senden. Diese Person kann die Abfragen dann in ein Abfrageverzeichnis auf einem anderen Webserver speichern und in eine andere Datenbank importieren.

So exportieren Sie eine Abfrage

Führen Sie die folgenden Schritte aus, während Sie mit einer Datenbank verbunden sind, in der sich die zu exportierende Abfrage befindet.

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Abfragen**.
2. Klicken Sie auf der Seite **Benutzerdefinierte Abfragen** auf den Namen der zu exportierenden Abfrage. Klicken Sie in der Symbolleiste auf die Schaltfläche **Bearbeiten**.
3. Klicken Sie auf der Seite **Abfrage bearbeiten** auf die Symbolleistenschaltfläche **Exportieren**. Die Seite **Abfrage exportiert** wird angezeigt.
4. Um das XML-Dokument für die Abfrage anzuzeigen, klicken Sie auf den Link für das XML-Dokument.
5. Um das XML-Dokument zu speichern, klicken Sie mit der rechten Maustaste auf den Link und wählen **Ziel speichern unte**r aus. Geben Sie einen Speicherort für die Datei an.

So importieren Sie eine Abfrage

Führen Sie die folgenden Schritte aus, während Sie mit der Datenbank verbunden sind, in die Sie eine Abfrage importieren möchten.

Wenn Sie eine Abfrage wieder zurück in eine Datenbank importieren möchten, muss sich die Abfrage in dem Abfrageverzeichnis befinden, das vom Webserver erkannt wird. Dieses Verzeichnis lautet standardmäßig c:\inetpub\wwwroot\LANDesk\LDMS\queries.

1. Klicken Sie in der Toolbox der Webkonsole auf **Berichte > Abfragen**.
2. Klicken Sie auf der Seite **Benutzerdefinierte Abfragen** auf die Symbolleistenschaltfläche **Neu**.
3. Klicken Sie auf der Seite **Abfrage bearbeiten** auf die Symbolleistenschaltfläche **Importieren**.
4. Wählen Sie die Abfrage aus, die Sie importieren möchten. Wenn Sie die Parameter dieser Abfrage vor dem Importieren überprüfen möchten, klicken Sie auf die Symbolleistenschaltfläche **Ansicht**.
5. Klicken Sie auf **Importieren**, um die Abfrage zu importieren. Wenn Sie alle Abfragen in der Liste Importieren möchten, klicken Sie auf **Alle importieren**.

Erstellen von LDAP-Abfragen mit dem Verzeichnis-Manager [Webkonsole]

Sie können nicht nur Datenbankabfragen für die Coredatenbank ausführen, sondern auch das Extra **Verzeichnis-Manager** verwenden, um unter Verwendung des Lightweight Directory Access Protocol (LDAP) nach Geräten in anderen Verzeichnissen zu suchen, auf diese Geräte zuzugreifen und sie als Zielgeräte auszuwählen.

Sie können Geräte auch auf der Basis von Attributen wie Prozessortyp oder Betriebssystem abfragen. Die Abfrage kann auch auf bestimmten Benutzerattributen wie Personalnummer oder Abteilung basieren.

Hinzufügen eines LDAP-Verzeichnisses

Damit Sie ein LDAP-Verzeichnis verwalten können, müssen Sie es zur Verzeichnis-Manager-Liste hinzufügen. Hierzu müssen Sie den Speicherort des Verzeichnisses in Ihrem Netzwerk kennen und über Anmeldeinformationen für den Zugriff auf dieses Verzeichnis verfügen.

So fügen Sie ein LDAP-Verzeichnis zum Verzeichnis-Manager hinzu

1. Klicken Sie in der Toolbox der Webkonsole auf **Verteilung > Verzeichnis-Manager**.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neues Verzeichnis**.

3. Geben Sie die URL für den Zugriff auf das Verzeichnis ein. Sie müssen das "LDAP://" am Anfang der URL nicht eingeben.
4. Geben Sie einen Benutzernamen und ein Kennwort für den Zugriff auf das Verzeichnis ein.
5. Klicken Sie auf **OK**.

Das Verzeichnis wird mit einem Baumsymbol im Extrabereich des Verzeichnis-Managers angezeigt. Sie können das Verzeichnis auch auswählen und auf die Schaltfläche **Bearbeiten** in der Symbolleiste klicken, um dessen Eigenschaften anzuzeigen.

Anzeigen von LDAP-Verzeichnissen

Wenn Sie mindestens ein Verzeichnis hinzugefügt haben, können Sie die Elemente in diesem Verzeichnis in der Strukturansicht **Verzeichnis-Manager**, die alle registrierten Verzeichnisse und Benutzer anzeigt, einsehen.

Der Aktionsbereich weist zwei Registerkarten auf: **LDAP-Zielliste** und **LDAP-Abfragen**. Klicken Sie darauf, um die von Ihnen als Ziele gewählten LDAP-Objekte und von Ihnen definierten LDAP-Abfragen anzuzeigen.

LDAP-Zielobjekte definieren

Sie können Objekte in der Verzeichnis-Manager-Struktur auswählen und als Ziele definieren. Die in diesen LDAP-Objekten enthaltenen Geräte können als Ziele für eine Aktion ausgewählt werden, die Sie für diese ausführen möchten, beispielsweise eine Softwareverteilung oder Patch- und Compliancescans.

So definieren Sie LDAP-Zielobjekte

1. Klicken Sie in der Toolbox der Webkonsole auf **Verteilung > Verzeichnis-Manager**.
2. Durchsuchen Sie die Struktur **Verzeichnis-Manager** und wählen Sie ein Objekt im LDAP-Verzeichnis aus.
3. Wählen Sie ein oder mehrere Elemente aus der Liste **Verzeichnisressourcen** aus und klicken Sie in der Symbolleiste auf die Schaltfläche **LDAP-Ziele**.
4. Wählen Sie das Extra aus, das Sie auf die Zielcomputer anwenden möchten. Die von Ihnen als Ziele definierten Elemente werden unter der Option **Zielliste** des Extras angezeigt.

Erstellen von LDAP-Verzeichnisabfragen

Sie können eine Abfrage erstellen, die Ergebnisse für ein Verzeichnisobjekt zurückgibt, beispielsweise für eine Stammorganisation (o), eine Domänenkomponente (dc) oder eine Organisationseinheit (ou).

So erstellen Sie eine LDAP-Abfrage

1. Klicken Sie in der Toolbox der Webkonsole auf **Verteilung > Verzeichnis-Manager**.
2. Durchsuchen Sie die Struktur **Verzeichnis-Manager** und wählen Sie ein Objekt im LDAP-Verzeichnis aus. Die von Ihnen erstellte Abfrage gibt von diesem Punkt in der Struktur ausgehend nach unten Ergebnisse aus.
3. Klicken Sie in der Symbolleiste auf die Schaltfläche **Neue LDAP-Abfrage**.
4. Geben Sie einen aussagekräftigen Namen für die Abfrage ein.
5. Wählen Sie ein LDAP-Attribut aus, das als Kriterium für die Abfrage dienen soll.
6. Klicken Sie auf einen Vergleichsoperator für die Abfrage (=,<=, >=) und auf einen Wert für das Attribut. Wenn Sie **Enthält** oder **Existiert** wählen, ist kein Wert erforderlich.

7. Bei einer komplexen Abfrage wählen Sie **UND** oder **ODER**, um die Anweisung mit der nächsten Anweisung zu verknüpfen.
8. Klicken Sie auf **Einfügen**, um die Anweisung hinzuzufügen.
9. Wiederholen Sie die Schritte 5 bis 8, um weitere Anweisungen zu erstellen.
10. Um eine Anweisung zu negieren, wählen Sie diese aus und klicken auf **NICHT**. Um eine Anweisung zu löschen, wählen Sie diese aus und klicken auf **Löschen**.
11. Wenn die Abfrage fertiggestellt ist, klicken Sie auf **Testen**, um zu prüfen, ob die Abfrage Ergebnisse zurückgibt.
12. Möchten Sie die Abfrage bearbeiten und hierbei LDAP-Syntax in freiem Format verwenden, klicken Sie auf **Erweitert**. Die Abfrage wird in einem Bearbeitungsfenster geöffnet, in dem Sie beliebige Syntaxoptionen verwenden können.
13. Wenn Sie fertig sind, klicken Sie auf **Speichern**. Die gespeicherte Abfrage erscheint auf der Registerkarte **LDAP-Abfragen** im Aktionsbereich des Verzeichnis-Managers.

Informationen zum Dialogfeld "Erweiterte LDAP-Abfrage"

Klicken Sie im Dialogfeld "Einfache LDAP-Abfrage" auf **Erweitert**, um das Dialogfeld "Erweiterte LDAP-Abfrage" zu öffnen. Das Dialogfeld "Erweiterte LDAP-Abfrage" wird ebenfalls angezeigt, wenn Sie eine bereits erstellte Abfrage bearbeiten.

- **Name:** Gibt den Namen der LDAP-Abfrage an. Bearbeiten Sie den Namen, um eine Kopie einer bestehenden Abfrage zu erstellen.
- **LDAP-Abfragestamm:** Zeigt das Stammobjekt im Verzeichnis zu dieser Abfrage an. Die von Ihnen erstellte Abfrage gibt von diesem Punkt in der Struktur ausgehend nach unten Ergebnisse aus.
- **LDAP-Abfrage:** Erstellt eine LDAP-Abfrage im freien Format.
- **Testen:** Klicken Sie hier, um die von Ihnen erstellte Abfrage zu testen.

Informationen zum Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) ist ein dem Industriestandard entsprechendes Protokoll für den Zugriff auf und die Anzeige von Informationen über Benutzer und Geräte. LDAP ermöglicht Ihnen die Organisation und Speicherung dieser Informationen in einem Verzeichnis. Ein LDAP-Verzeichnis ist insofern dynamisch, als dass es ggf. aktualisiert werden kann. Es wird verteilt, wodurch ein Schutz vor einem zentralen Ausfall gegeben ist.

Die nachstehenden Beispiele beschreiben LDAP-Abfragen, die zum Durchsuchen des Verzeichnisses verwendet werden können:

- Alle Einträge abrufen: (objectClass=*)
- Einträge abrufen, die 'bob' an irgendeiner Stelle des Namens enthalten: (cn=*bob*)
- Einträge mit einem allgemeinen Namen abrufen, die größer/gleich 'bob' sind: (cn>='bob')
- Alle Benutzer mit einem E-Mail-Attribut abrufen: (&(objectClass=user (email=*)
- Alle Benutzereinträge mit einem E-Mail-Attribut und einem Nachnamen abrufen, der 'Schmidt' entspricht: (&(sn=Schmidt (objectClass=user (email=*)
- Alle Benutzereinträge mit einem Namen abrufen, der mit 'Andrea', 'Chris' oder 'Micha' beginnt: (& (objectClass=User (| (cn=Andrea* (cn=Chris* (cn=Micha*)
- Alle Benutzer ohne E-Mail-Attribut abrufen: (!(email=*)

Die formale Definition des Suchfilters ist wie folgt (von RFC 1960):

- <filter> ::= '(' <filtercomp> ')'
- <filtercomp> ::= <and> | <or> | <not> | <item>
- <and> ::= '&' <filterlist>
- <or> ::= '|' <filterlist>
- <not> ::= '!' <filter>
- <filterlist> ::= <filter> | <filter> <filterlist>
- <item> ::= <simple> | <present> | <substring>
- <simple> ::= <attr> <filtertype> <value>
- <filtertype> ::= <equal> | <approx> | <ge> | <le>
- <equal> ::= '='
- <approx> ::= '~='
- <ge> ::= '>='
- <le> ::= '<='
- <present> ::= <attr> '=*'
- <substring> ::= <attr> '=' <initial> <any> <final>
- <initial> ::= NULL | <value>
- <any> ::= '*' <starval>
- <starval> ::= NULL | <value> '*' <starval>
- <final> ::= NULL | <value>

Das Token <attr> ist eine Zeichenfolge, die einen Attributtyp repräsentiert. Das Token <value> ist eine Zeichenfolge, die einen Attributwert repräsentiert, dessen Format vom zugrunde liegenden Verzeichnisdienst definiert wird.

Wenn ein <value> eines der folgenden Zeichen * oder (or) enthalten muss, stellen Sie den Backslash (\) vor das Zeichen.

Verwalten von Inventar [Webkonsole]

Sie können Inventarscans verwenden, um die Hardware- und Softwaredaten für verwaltete Geräte anzuzeigen. Inventardaten werden in der Coredatenbank gespeichert. Hierzu gehören Informationen zu Hardware, Gerätetreibern, Software, Speicher und Umgebung. Die Inventardaten sind beim Verwalten und Konfigurieren von Geräten hilfreich. Außerdem können Sie damit schnell Systemprobleme erkennen.

Sie können Inventardaten anzeigen, drucken und exportieren. Sie können mit dem Inventarscanner zudem Abfragen definieren, Server zu Gruppen zusammenfassen und benutzerdefinierte Berichte generieren.

Übersicht über das Inventarscannen

Wenn Sie ein Gerät mit einem LANDesk Management-Agenten konfigurieren, gehört der Inventarscanner zu den auf dem Gerät installieren Komponenten. Beim Erstellen einer Agentenkonfiguration können Sie angeben, wann der Inventarscanner auf dem Gerät ausgeführt werden soll.

Der Inventarscanner wird beim erstmaligen Konfigurieren des Geräts automatisch ausgeführt. Der Name der Scanner-Programmdatei lautet für Windows ldiscn32.exe und für Linux ldiscan. Der Inventarscanner erfasst Hardware- und Softwaredaten und fügt sie in die Coredatenbank ein. Im Anschluss daran wird der Hardwarescan in dem von Ihnen angegebenen zeitlichen Abstand ausgeführt (standardmäßig ist dies einmal pro Tag).

So konfigurieren Sie Softwarescaneinstellungen

1. Klicken Sie auf dem Coreserver auf **Start > Alle Programme > LANDesk > LANDesk - Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte **Inventar**.
3. Um die Frequenz der Softwarescans zu ändern, klicken Sie auf **Software**.
4. Nehmen Sie bei Bedarf weitere Änderungen vor. (Klicken Sie auf **Hilfe**, um Beschreibungen der Optionen anzuzeigen.)
5. Wenn Sie fertig sind, klicken Sie auf **OK**.

Nach dem ersten Scan kann der Inventarscanner von der Konsole aus als geplanter Task ausgeführt werden. Um einen Inventarscan auf Remoteservern planen zu können, muss auf diesen Geräten der Standard Management Agent laufen.

HINWEIS: Ein Gerät, das über das Extra **Erkennung nicht verwalteter Geräte** zur Coredatenbank hinzugefügt wurde, hat seine Inventardaten noch nicht in die Coredatenbank gescannt. Sie müssen einen Inventarscan auf jedem Gerät ausführen, damit die gesamten Inventardaten für dieses Gerät angezeigt werden.

Sie können Inventardaten anzeigen lassen und wie folgt verwenden:

- die Spalten in der Liste **Alle Geräte** anpassen, um bestimmte Inventarattribute anzuzeigen
- die Coredatenbank nach Geräten mit bestimmten Inventarattributen durchsuchen
- Geräte gruppieren, um Verwaltungstasks wie die Softwareverteilung zu beschleunigen
- spezielle Berichte basierend auf Inventarattributen generieren
- Hardware- und Softwareänderungen auf Geräten verfolgen und Alarme oder Protokolleinträge generieren, wenn solche Änderungen stattfinden.

Deltascannen

Nach dem ersten vollständigen Scan auf einem Windows-Gerät erfasst der Inventarscanner bei nachfolgenden Scans nur Deltaänderungen und sendet diese an die Coredatenbank. Verwenden Sie die Scanneroption /RSS zum Abrufen von Softwareinformationen aus der Windows-Registrierung. (Diese Option gilt nicht für Linux-Geräte.)

Erzwingen eines vollständigen Scans

Wenn Sie einen vollständigen Scan der Hardware- und Softwaredaten eines Windows-Geräts erzwingen möchten, können Sie die vorhandene Deltascandatei löschen und die entsprechende Einstellung in "Dienste konfigurieren" ändern. (Diese Option gilt nicht für Linux-Geräte.)

1. Löschen Sie die Datei **invdelta.dat** auf dem Gerät. Eine Kopie des letzten Inventarscans ist lokal als verborgene Datei mit dem Namen "invdelta.dat" gespeichert. Die Umgebungsvariable LDMS_LOCAL_DIR legt den Pfad dieser Datei fest. Standardmäßig ist dies das Verzeichnis C:\Programme\LANDesk\LDClient\Data.
2. Fügen Sie die Option **/sync** in die Befehlszeile des Inventarscanners ein. Um die Befehlszeile zu bearbeiten, klicken Sie auf **Start > Alle Programme > LANDesk Management**, klicken mit der rechten Maustaste auf das Verknüpfungssymbol **Inventarscan**, wählen **Eigenschaften > Verknüpfung** aus und bearbeiten dann den **Zielpfad**.

3. Klicken Sie auf dem Coreserver auf **Start > Alle Programme > LANDesk > LANDesk - Dienste konfigurieren**.
4. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
5. Klicken Sie auf die Einstellung **Do Delta**. Geben Sie in das **Wert**-Feld **0** ein.
6. Klicken Sie zweimal auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Scankomprimierung

Inventarscans mit dem Windows-Inventarscanner ldiscn32.exe werden standardmäßig komprimiert. Der Scanner komprimiert vollständige und Deltascans in einem Komprimierungsverhältnis von ca. 8:1. Scans werden zunächst vollständig im Speicher erstellt, dann komprimiert und mithilfe eines größeren Pakets an den Coreserver gesendet. Die Scankomprimierung reduziert die Anzahl der erforderlichen Pakete und die Bandbreitennutzung. (Die Scankomprimierung kommt auf Linux-Geräten nicht zur Anwendung.)

Scanverschlüsselung

Inventarscans auf Windows-Geräten sind verschlüsselt (nur TCP/IP-Scans). Sie können die Inventarscanner-Verschlüsselung deaktivieren, indem Sie eine Einstellung in "Dienste konfigurieren" ändern.

1. Klicken Sie auf dem Coreserver auf **Start > Alle Programme > LANDesk > LANDesk - Dienste konfigurieren**.
2. Klicken Sie auf die Registerkarte **Inventar** und klicken Sie dann auf **Erweiterte Einstellungen**.
3. Klicken Sie auf die Einstellung **Verschlüsselung deaktivieren**. Geben Sie in das **Wert**-Feld **1** ein.
4. Klicken Sie auf **Festlegen** und klicken Sie dann auf **OK**.
5. Klicken Sie auf **OK** und klicken Sie dann auf **Ja**, wenn die Eingabeaufforderung zum Neustart des Dienstes angezeigt wird.

Anzeigen von Inventardaten

Sobald ein Gerät vom Inventarscanner gescannt wurde, können Sie dessen Systeminformationen in der Konsole anzeigen.

- Anzeigen einer Inventarübersicht
- Anzeigen des kompletten Inventars
- Anzeigen von Attributeigenschaften
- Anzeigen von Systeminformationen

Darüber hinaus können Inventardaten auch in von Ihnen generierten Berichten angezeigt werden.

Anzeigen der Inventarzusammenfassung von der Echtzeitinventar-Konsole aus

Die Inventarübersicht auf der Seite **Übersicht** in der Serverinformationskonsole bietet einen schnellen Überblick über die Betriebssystemkonfiguration sowie Systeminformationen des Geräts.

HINWEIS: Wenn Sie ein Gerät mithilfe des Erkennungstool in die Coredatenbank eingefügt haben, sind seine Inventardaten noch nicht in die Coredatenbank gescannt. Sie müssen einen Inventarscan auf dem

Server ausführen, damit die Inventarübersicht erfolgreich erstellt werden kann.

So zeigen Sie eine Inventarübersicht an

1. Klicken Sie in der Netzwerkansicht der LANDesk Management-Konsole in einer **Geräte**gruppe mit der rechten Maustaste auf ein Gerät und wählen Sie **Echtzeitinventar und Überwachung**.
2. Klicken Sie in der Toolbox auf **Systeminformationen > System - Übersicht**.

Übersichtsdaten

Diese Informationen werden eingeblendet, wenn Sie die Inventarübersicht für ein verwaltetes Gerät anzeigen.

- **Zustand:** Der aktuelle Zustand des Geräts.
- **Typ:** Der Gerätetyp.
- **Hersteller:** Der Hersteller des Geräts.
- **Modell:** Der Modelltyp der Geräts.
- **BIOS-Version:** Die ROM BIOS-Version.
- **Betriebssystem:** Das Windows- oder Linux-Betriebssystem, das auf dem Gerät ausgeführt wird.
- **BS-Version:** Die Versionsnummer des Betriebssystems auf dem Gerät.
- **CPU:** Auf dem Gerät ausgeführte(r) Prozessor bzw. Prozessoren.
- **Anfälligkeitsscanner:** Die Version des installierten Agenten.
- **Remotesteuerung:** Die Version des installierten Agenten.
- **Softwareverteilung:** Die Version des installierten Agenten.
- **Inventarscanner:** Die Version des installierten Agenten.
- **Überwachung:** Die Version des installierten Überwachungsscanners
- **Letzter Neustart:** Zeitpunkt, zu dem das Gerät das letzte Mal neu gestartet wurde.
- **CPU-Nutzung:** Der Prozentsatz des Prozessors, der gegenwärtig genutzt wird.
- **Physikalischer Speicher belegt:** Auf dem Gerät verfügbarer RAM.
- **Virtueller Speicher verwendet:** Auf dem Gerät verfügbarer Speicher, einschließlich RAM und Speicher der Auslagerungsdatei.
- **Laufwerksspeicherplatz belegt:** Zurzeit belegter Speicherplatz (in %). Wenn Sie mehrere Festplattenlaufwerke besitzen, wird jedes Laufwerk einzeln aufgeführt.

IPMI-fähige Geräte zeigen zusätzliche IPMI-spezifische Daten an. Für Linux-Geräte werden ähnliche Informationen in der **Übersicht** angezeigt.

Anzeigen des kompletten Inventars

Ein vollständiges Inventar umfasst eine komplette und ausführliche Aufstellung der Hardware- und Softwarekomponenten eines Geräts. Die Aufstellung enthält Objekte und Objektattribute.

So zeigen Sie ein vollständiges Inventar an

1. Klicken Sie in der Netzwerkansicht der LANDesk Management-Konsole in einer **Geräte**gruppe mit der rechten Maustaste auf ein Gerät.

2. Wählen Sie in der Webkonsole im Extra **Eigene Geräte** eine Gruppe (beispielsweise "Eigene Geräte") aus und klicken Sie auf ein Gerät. Klicken Sie im Aktionsbereich auf die Registerkarte **Eigenschaften** und klicken Sie dann auf **Inventar anzeigen**.

Anzeigen von Attributeigenschaften

In der Inventarliste können Sie Attributeigenschaften für die Inventarobjekte eines Geräts anzeigen. Attributeigenschaften geben Aufschluss über die Eigenschaften und Werte eines Inventarobjekts. Sie können auch neue, angepasste Attribute erstellen und benutzerdefinierte Attribute bearbeiten.

So zeigen Sie die Eigenschaften eines Attributs an

1. Klicken Sie in der vollständigen Inventarliste auf das Attribut im linken Bereich. Unter Umständen müssen Sie Elemente erweitern, um das von Ihnen gesuchte Attribut zu finden.
2. Zum Ausdrucken der Informationen verwenden Sie die Funktion **Drucken** Ihres Browsers.

Anzeigen von Systeminformationen

Von der Konsole "Echtzeitinventar und Überwachung" aus können Sie die Systeminformationen des Geräts anzeigen und ändern. Informationen in den Kategorien **Hardware**, **Protokolle, Software** und **Sonstige** sind entweder gespeicherte Daten oder Echtzeitdaten. Sobald Sie auf eine Informationsverknüpfung klicken, können Sie detaillierte Informationen zu der ausgewählten Komponente anzeigen und ggf. Grenzwerte definieren und Informationen eingeben.

1. Doppelklicken Sie in der Ansicht **Alle Geräte** der Webkonsole auf ein Gerät.
2. Klicken Sie in der Toolbox auf **Systeminformationen**.
3. Erweitern Sie die Gruppe und klicken Sie auf die Informationsverknüpfung, die Sie anzeigen möchten.

Konfigurieren von Rollup-Datenbanklinks [Webkonsole]

In diesem Abschnitt wird beschrieben, wie Datenbanklinks in den LANDesk Software-Rollup-Szenarien konfiguriert werden. Dies sind die Szenarien:

- Oracle-Rollup auf Oracle
- SQL Server-Rollup auf SQL Server

Die mit dieser Konfiguration beauftragte Person benötigt darüber hinaus Zugriff auf alle von LANDesk verwendeten Datenbankverwaltungssysteme (DBMS) und muss Sicherheitsberechtigungen zum Erstellen von Datenbanklinks und Ausführen von Konfigurationsschritten auf DBMS-Serverebene besitzen.

Oracle-Rollup auf Oracle

Konfigurieren der Oracle-Datenbank

Die Datei "TNSNames.ora" auf dem Datenbankserver, in dem sich Ihre Rollup-Datenbank befindet, muss einen Eintrag für Ihre Coreserver-Datenbank enthalten.

1. Melden Sie sich für eine Oracle-Datenbank innerhalb der Enterprise Manager Console bei Ihrer Datenbank an. Erweitern Sie **Verteilt**.
2. Klicken Sie im Kontextmenü des Elements **Datenbankverknüpfungen** auf **Erstellen**.

3. Geben Sie im Feld **Name** einen Namen für Ihren Datenbanklink ein.
   Hinweis: Wenn die AR-Datenbank Oracle9i verwendet, ist als Linkname jeder noch nicht benutzte oder reservierte Name zulässig. Das Installationsprogramm fordert Sie zur Eingabe dieser Informationen auf.
4. Wählen Sie **Fester Benutzer** aus und geben Sie einen Benutzernamen und ein Kennwort für die Datenbank des Coreservers ein.
5. Geben Sie in das Feld **Dienstname** den TNSNames.ora-Eintrag (d. h. NetAlias) ein, der auf Ihre Coreserver-Datenbank verweist.
6. Klicken Sie auf **Erstellen**.
7. Doppelklicken Sie auf Ihren neu erstellten Link und klicken Sie auf **Testen**. Sie sollten eine Nachricht erhalten, die bestätigt, dass der Link aktiv ist. Sie können Ihren Link außerdem testen, indem Sie sich bei der Rollup-Datenbank anmelden und folgenden Befehl eingeben:

   Select count(*) from computer@linkname;

   Wenn daraufhin eine Aufzählung der Geräte in der Produktionsdatenbank des Coreservers zurückgegeben wird, so bedeutet dies, dass der Link ordnungsgemäß konfiguriert wurde.

SQL Server-Rollup auf SQL Server

Konfigurieren der SQL Server-Datenbank

1. Öffnen Sie SQL Server Management Studio.
2. Erweitern Sie sowohl Ihren Server als auch **Serverobjekte**.
3. Klicken Sie im Kontextmenü des Elements **Verknüpfte Server** auf **Neue verknüpfte Server**.
4. Führen Sie auf der Seite **Allgemein** die Schritte 5 - 11 aus:
5. **Verbindungsserver**: Geben Sie einen eindeutigen Namen für diesen Datenbanklink ein (z. B. LDMS core server1-Link).
6. Wählen Sie **Andere Datenquelle** aus.
7. Wählen Sie **Microsoft OLE DB Provider für SQL Server** aus.
8. **Produktname**: Geben Sie LDMS ein.
9. **Datenquelle**: Geben Sie den Namen des Datenbankservers ein, auf dem sich die Coredatenbank befindet.
10. **Providerzeichenfolge** bzw. Anbieterzeichenfolge: Geben Sie die Zeichenfolge des Providers ein. Zum Beispiel:

    SQL Server
    provider=SQLOLEDB.1;user id=<Benutzer für die Datenbank des Coreservers>
    ** *Der Abschnitt "user id" der Provider-Zeichenfolge wird im Connection-String für die Verbindung mit einer anderen SQL Server-Datenbank benötigt.* **

11. **Katalog**: Geben Sie den physikalischen Namen der Datenbank Ihres Coreservers ein (z. B. lddb).
12. Wählen Sie auf der Seite **Sicherheit** die Option **In folgendem Sicherheitskontext verwendet** aus, geben Sie den Benutzernamen und das Kennwort für die Datenbank des Coreservers ein und klicken Sie dann auf **OK**.

13. Klicken Sie auf **Neue Abfrage** und geben Sie den folgenden Befehl ein:

    Select count(*) from [Linkname].[Datenbankname].[Name des Tabelleneigentümers].Computer

    Bei Verwendung der obigen Werte würde diese Abfrage wie folgt angezeigt:

    Select count(*) from [LDMS Coreserver1-Link].[lddb].[dbo].Computer

    Wenn die korrekte Anzahl zurückgegeben wird, wurde der Link ordnungsgemäß eingerichtet.

Multi-Core-Unterstützung [Webkonsole]

Die folgenden Bedingungen müssen erfüllt sein, damit die Verwendung mehrerer Cores unterstützt wird:

- Beide Cores müssen derselben Domäne angehören.
- Das Domänenadministratorkonto muss auf beiden Cores zur lokalen LANDesk ManagementSuite-Benutzergruppe hinzugefügt werden.
- Die Identität der LANDesk COM+-Anwendung unter Komponentendienste muss auf den Domänenadministrator festgelegt sein. Dieser Vorgang wird im nächsten Abschnitt beschrieben.
- Die Datei "core.asp" muss so bearbeitet werden, dass sie den zweiten Core beinhaltet. Die Datei core.asp befindet sich im Ordner \inetpub\wwwroot\LANDesk\LDMS\xml. Sobald dies geschehen ist, sehen Sie beim ersten Zugriff auf die Webkonsole in einem Browser eine Dropdownliste, in der die in core.asp definierten Server enthalten sind. Klicken Sie auf den gewünschten Server und klicken Sie auf **Verbinden**.

Nachstehend finden Sie ein Beispiel für eine core.asp, die mehrere Server enthält.

```
<?xml version="1.0" ?>
<core>
<cores>
<item name="Core_Host_Name_1" rollup="0"/>
<item name="Core_Host_Name_2" rollup="0"/>
<item name="Rollup_Core_Host_Name_3" rollup="1"/>
</cores>
</core>
```

So melden Sie sich bei einem Core in einer Umgebung mit mehreren Cores an

1. Starten Sie die Management Suite Webkonsole.
2. Wählen Sie in der Liste **Core auswählen** den Core aus, bei dem Sie sich anmelden möchten und klicken Sie dann auf **Verbinden**. Geben Sie den Benutzernamen und das Kennwort ein.

Hinweise

- Damit die Clientkonfiguration erfolgreich erstellt wird, müssen Sie die korrekte URL für den Core verwenden. Andernfalls ist die Konfiguration nicht funktionsfähig.
- Möglicherweise erweist es sich als hilfreich, Einträge für jeden Coreserver in Ihr **Favoriten**-Menü in Ihrem Browser einzufügen. Das erleichtert das Umschalten zwischen Cores.

Konfigurieren von COM+-Serveranmeldeinformationen

Wenn Sie einen Webkonsolenserver verwenden möchten, der sich nicht auf dem Core befindet, oder wenn Sie Domänengruppen innerhalb der LANDesk Management Suite-Gruppe auf dem Coreserver verwenden möchten, müssen Sie zusätzliche Schritte zum Konfigurieren des Servers ausführen, damit die Management Suite Authentifizierung ordnungsgemäß arbeitet. Remote-Webkonsolenserver müssen Datenbankverbindungsinformationen und Benutzerinformationen aus dem Coreserver abrufen; da Remote-Webkonsolenserver jedoch per "Identitätswechsel" angenommene Web-Anmeldeinformationen auf IIS (Internet Information Services) verwenden, können sie nicht direkt mit dem Coreserver kommunizieren.

Webkonsolenserver und Coreserver lösen dieses Problem, indem sie eine COM+-Anwendung verwenden, um über HTTPS zu kommunizieren; auf diese Weise kann der Webkonsolenserver Coreserver-Datenbankinformationen und -Benutzerinformationen abrufen. Sie müssen diese COM+-Anwendung auf dem Webkonsolenserver für die Verwendung eines Kontos konfigurieren, das über die erforderlichen Rechte verfügt, beispielsweise das Domänenadministratorkonto. Das von Ihnen bereitgestellte Konto muss sich in der LANDesk Management Suite-Gruppe auf dem Coreserver befinden (auf diese Weise erhält es Zugriff auf die Datenbankverbindungsinformationen des Coreservers) und muss Rechte zum Aufzählen von Windows-Domänenmitgliedern besitzen.

Wenn Sie Domänengruppen in der LANDesk Management Suite-Gruppe des Coreservers verwenden, muss Management Suite zudem in der Lage sein, Windows-Domänenmitglieder aufzuzählen. In diesem Fall müssen Sie außerdem ein Konto für die LANDesk1 COM+-Anwendung des Coreservers bereitstellen.

So konfigurieren Sie die LANDesk1 COM+-Anwendung auf einem Coreserver oder Remote-Webkonsolenserver

1. Navigieren Sie zu dem Webserver oder Coreserver, den Sie konfigurieren möchten.
2. Öffnen Sie in der Windows-Systemsteuerung die "Verwaltung" und anschließend **Komponentendienste**.
3. Klicken Sie auf **Komponentendienste > Computer > Arbeitsplatz > COM+-Anwendungen**.
4. Klicken Sie mit der rechten Maustaste auf die **LANDesk1** COM+-Anwendung und wählen Sie dann **Eigenschaften**.
5. Geben Sie auf der Registerkarte **Identität** die Anmeldeinformationen ein, die Sie verwenden möchten.
6. Klicken Sie auf **OK**.

Inventory Manager

LANDesk Inventory Manager

LANDesk Inventory Manager ist eine Version von LANDesk Management Suite 9, die nur die folgenden inventarbezogenen Funktionen enthält:

- Inventarscans und inventarbezogene Konsolenfunktionen
- Benutzerdefinierte Datenformulare
- Softwarelizenzüberwachung
- Erkennung nicht verwalteter Geräte
- Berichte für die oben genannten Funktionen

Die Inventory Manager-Installation auf einem Coreserver beinhaltet alle Management Suite 9-Komponenten. Wenn Sie jedoch einen Coreserver mit einem Konto aktivieren, das für Inventory Manager lizenziert ist, sind die Nicht-Inventory Manager-Funktionen in der Konsole von Management Suite und in Webkonsole weder verwendbar noch sichtbar.

Informationen zur Verwendung von Inventory Manager finden Sie in den Abschnitten, deren Titel den Funktionen in der obigen Liste entsprechen. Im Allgemeinen lässt sich leicht erkennen, welche Informationen für Inventory Manager nicht von Belang sind. Es handelt sich dabei meist um Abschnitte, in denen Management Suite Funktionen wie Softwareverteilung und Remotesteuerung beschrieben werden, die nicht Teil von Inventory Manager sind.

HP Hardware Management

LANDesk plus HP Hardware and Software Management – Übersicht

Das Extra LANDesk Management Suite plus HP Hardware and Software Management ist eine integrierte Partnerlösung für Ihre LANDesk® Management Suite bzw. LANDesk Security Suite Netzwerkumgebung. Mit LANDesk plus HP Management können Sie Ihre HP Geräte und zugehörigen Retail Point-of-Sale (RPOS)-Peripheriegeräte für den Einzelhandel von einer zentralen Konsole aus verwalten.

Die Lösung kombiniert die HP Management-Funktionen mit den leistungsstarken Extras von LANDesk Management Suite. So können LANDesk Administratoren verwaltete HP Geräte einfach und effizient scannen, Daten zu Komponenten des LANDesk Inventars anzeigen (sowohl zu Hardware als auch zu Software), Abfragen durchführen, die neuesten HP Updates bereitstellen und installieren, Zustandsalarme konfigurieren und Berichte generieren.

Diese integrierte Funktionalität in Verbindung mit den LANDesk Extras für die Alarmierung und Berichterstellung hilft LANDesk Administratoren, die Nutzung von Retail POS-Peripheriegeräten, Grenzwertüberschreitungen und Fehler bei der Hardware, den Stromverbrauch und die Leistung, den Batteriezustand, den Verbindungsstatus von HP Netzwerkkarten, Wartungsprobleme, fehlende Geräte usw. zu erkennen und entsprechend zu reagieren.

Neuerungen bei der Updateversion HP 1.4

Die HP Version 1.4 von LANDesk plus HP Management bietet zusätzlich Unterstützung für *HP Thin Client Management*. Zur Erkennung, Konfiguration, Verwaltung und für den Schutz von HP Thin Client-Geräten in Ihrem Netzwerk stehen mehrere nützliche LANDesk Management Suite- und Security Suite-Extras zur Verfügung.

LANDesk Management Suite Version 9.5 bietet Unterstützung für die folgenden HP Thin Client-Plattformen:

- Windows Embedded Standard 7 Enterprise (WES7)
- Windows Embedded Standard 09 Enterprise (WES09)
- HP ThinPro Linux Ubuntu

WICHTIG: LDMS 9.5 umfasst die neusten HP Software and Hardware Management-Funktionen
Die neuen HP 1.4 Funktionen – HP Thin Client Management-Extras – sind standardmäßig ab der Freigabe von LANDesk Management Suite Version 9.5 mit in das Produkt eingeschlossen. Dies bedeutet, dass Sie beim Download und bei der Installation von LDMS 9.5 sämtliche Funktionen der Vorgängerversionen HP 1.2, 1.3 und zusätzlich 1.4 erhalten. Es ist NICHT nötig, diese vorherigen HP Versionen separat zu installieren.

LANDesk plus HP Thin Client Management bietet die folgenden LANDesk Extras und Funktionen:

- Erkennung nicht verwalteter Geräte
- Agentenkonfiguration
- Versorgung: Abbilderfassung- und -bereitstellung
- Schreibfilterverwaltung (NUR für WES-Plattformen)
- Softwareverteilung

- Patchmanagement
- Remotesteuerung
- Inventaransicht

Weitere Informationen über die HP Thin Client-Verwaltung finden Sie unter "Verwalten von HP Thin Client-Geräten über die LANDesk Konsole" auf Seite 1028.

Neuerungen bei der Updateversion HP 1.3

Die HP Version 1.3 bietet zusätzlich Verwaltungsfunktionen für HP *Software*. Das Produkt trägt jetzt den Namen **LANDesk Management Suite plus HP Software and Hardware Management**.

Systemadministratoren können jetzt integrierte HP Extras zur Überwachung und Verwaltung zusätzlicher softwarespezifischer Funktionen ihrer verwalteten HP Geräte verwenden.

Die neu hinzugefügten Extras für die HP Verwaltung umfassen:

- **HP Power Assistant:** Mit diesem Extra können Sie den Energieverbrauch bei Ihren HP Geräten überwachen und steuern. Verwenden Sie angepasste Energieeinstellungen und stellen Sie diese für HP Zielgeräte zur Optimierung des Energieverbrauchs und der Leistung bereit. Die HP Power Assistant-Daten sind über das Geräteinventar und über vordefinierte Berichte abrufbar.
- **HP Battery Check**: Diese Extra scannt Ihr verwaltetes HP Gerät automatisch und gibt Ihnen die Möglichkeit, den Batteriezustand des Geräts zu verfolgen. Die HP Battery Check-Daten sind über das Geräteinventar und über vordefinierte Berichte abrufbar.
- **HP Connection Manager**: Dieses Extra scannt Ihre verwalteten HP Geräte automatisch, prüft den Status der HP kompatiblen Netzwerkkarte und meldet diese Informationen an die Coredatenbank weiter. Diese Informationen können Sie zur Aktivierung einer Netzwerkkarte verwenden und auf diese Weise die Netzwerk- bzw. Internet-Konnektivität und -Aktivität verfolgen und verwalten.
- **HP Softwarerichtlinien**: Dieses neue Extra (im Extra-Fenster **Sicherheitskonfigurationen**) verwenden Sie, um auf der Basis von HP Power Assistant-Einstellungen benutzerdefinierte Richtlinien zu erstellen, die Sie dann mit Hilfe eines Tasks zum Ändern von Einstellungen und dem Extra "Geplante Tasks" für Ihre verwalteten Geräte bereitstellen können.

Sie können diese neuen Daten im Geräteinventar unterhalb des Komponentenknotens **Hewlett-Packard** anzeigen.

Ferner wurden die folgenden neuen Berichte zum LANDesk Extra "Berichte" hinzugefügt:

- HP Akkuzustandsüberprüfung
- HP Mobile Broadband-Karte - Assetinformationen
- HP Power Assistant - Energieverbrauch
- HP Power Assistant - Energieverbrauch in Bezug auf die verschiedenen Wochentage

Weitere Informationen zur HP Clientverwaltung finden Sie unter Verwalten von HP Geräten über die LANDesk Konsole.

Bereits mit der ersten Version HP 1.2 eingeführte Funktionen

HP 1.2 ist die erste freigegebene Version des Extras **LANDesk Management Suite plus HP Hardware Management**. Diese integrierte Lösung bieten Systemadministratoren folgenden Merkmale und Funktionen:

- Zugriff auf die integrierten HP Extras für die Geräteverwaltung in der LANDesk Konsole
- Konfigurieren von HP Geräten für die Geräteverwaltung (Scannen, Echtzeitinventar und Überwachung, Alarmfunktion, Berichte)
- Ausführen von Inventarscans auf HP Geräten
- Anzeigen der HP Geräteinventars (einschließlich der Retail POS-Geräte)
- Anzeigen des Echtzeitinventars und der Echtzeitüberwachung von HP Geräten
- Ausführen von Abfragen mit spezifischen Inventardaten für HP Gerätekomponenten
- Konfigurieren und Bereitstellen von HP BIOS-Einstellungen für HP Zielgeräte
- Konfigurieren und Bereitstellen von TPM (Trusted Platform Module)-Sicherheitschip-Einstellungen für HP Zielgeräte
- Ändern/Aktualisieren von BIOS- und TPM-Einstellungen mit dem Extra "Geplante Tasks"
- Bereitstellen und Installieren der neusten HP Updates (einschließlich HP Hardware- und Firmwareupdates)
- Konfigurieren von Zustandsalarmen für Ereignisse, Fehler, das Erreichen von Nutzungsgrenzwerten und anderen Attributen für verwaltete HP Geräte und Retail POS-Peripheriegeräte
- Generieren von Berichten, einschließlich Standardinventar- und BIOS-Berichten sowie vordefinierten Berichten für HP Geräte

Retail POS-Geräte

Zu den Retail POS-Geräten zählen:

- HP AP5000
- HP Kassenschublade
- HP Hybriddrucker mit MICR
- HP Imaging-Barcodescanner
- HP Tastatur
- HP Tastatur mit Magnetstreifen-Lesegerät
- HP Laser-Barcodescanner
- HP Mini-Magnetstreifen-Lesegerät
- HP Pole Line-Display
- HP RP5800
- HP Thermo-Kassenbondrucker
- und mehr...

Erste Schritte

Damit Sie die Extras für LANDesk Management Suite plus HP Hardware and Software Management verwenden können, müssen Sie zunächst das HP Softwarepaket installieren (NUR für LDMS Version 9.0 Coreserver) und die HP Geräte mit den erforderlichen LANDesk Agenten konfigurieren.

Als Ausgangspunkt sollten Sie sich die "Installationsvoraussetzungen" auf Seite 989 ansehen.

Zusätzliche Informationsquellen

Weitere Informationen zur Verwendung der Extras von LANDesk Management Suite finden Sie in den Hilfethemen zu LANDesk Management Suite.

Navigieren Sie im LANDesk Help Center in den Hilfethemen zu LANDesk Management Suite oder führen Sie eine Suche mit einem bestimmten Schlüsselwort oder Ausdruck durch, um die von Ihnen gewünschten Informationen zu finden.

Ausführliche Informationen zur Installation und Konfiguration eines LANDesk Coreservers finden Sie auf der Website der LANDesk Benutzercommunity in den BKM (Best Known Method)-Dokumenten zur Installation und Bereitstellung (*Installation and Deployment*).

HINWEIS: Die LANDesk Benutzercommunity
Die LANDesk Benutzercommunity bietet Benutzerforen und bewährte Methoden für alle LANDesk Produkte und Technologien. Diese wertvollen Ressourcen finden Sie unter http://community.landesk.com

Installationsvoraussetzungen

In diesem Abschnitt werden die Hardware- und Softwareanforderungen für die Installation von LANDesk plus HP Management und für die HP Geräte beschrieben, die über die LANDesk Konsole mit den integrierten HP Extras verwaltet werden sollen.

Die folgenden Voraussetzungen müssen erfüllt sein, bevor Sie die Extras "LANDesk Management Suite plus HP Hardware and Software Management" in Ihrer Netzwerkumgebung installieren, konfigurieren und verwenden können.

LANDesk Coreserver – Anforderungen

- **WICHTIG:** Windows Server 2008 R2 x64 als Coreservercomputer
- LDMS 9.0 Coreserver in der Version SP3 ist installiert (kann von der LANDesk Benutzercommunity heruntergeladen werden).

HINWEIS: Dokumente zur Installation und Konfiguration auf der LANDesk Benutzercommunity-Website
Wenn der LANDesk Coreserver noch nicht installiert ist, lesen Sie den Abschnitt "Installation" des folgenden Dokuments auf der LANDesk Benutzercommunity-Website: Community Document 7423.

Wenn Sie mit einem **LDMS 9.0-Coreserver** arbeiten, müssen Sie die HP Integrationssoftware installieren. Informationen hierzu finden Sie unter "Installieren der HP Hardware and Software Management-Software" auf Seite 990.

Wenn Sie mit einem **LDMS 9.5-Coreserver** arbeiten, müssen Sie die HP Installationssoftware nicht installieren. Jetzt haben Sie alle Vorbereitungen getroffen, um HP Clients und HP Thin Clients konfigurieren und über die LANDesk Konsole verwalten zu können. Weitere Informationen finden Sie unter "Konfigurieren von HP Geräten für LANDesk Verwaltungstasks" auf Seite 991.

HP Client – Anforderungen

Folgende Anforderungen werden an Standard HP-Clientgeräte gestellt:

- Eines der folgenden Betriebssysteme ist installiert: Windows XP, Windows Vista (32-Bit, 64-Bit) oder Windows 7 (32-Bit, 64-Bit). (**WICHTIG**: Das Extra für die HP TPM-Sicherheitschip-Einstellungen wird vom Betriebssystem Windows XP NICHT unterstützt.)
- Der Standard LANDesk Agent ist installiert (und für Alarmierung, Echtzeitinventar und Überwachung konfiguriert). Weitere Informationen finden Sie unter "Konfigurieren von HP Geräten für LANDesk Verwaltungstasks" auf Seite 991.

- CMI-Provider sind installiert. Dieses HP Update trägt die Bezeichnung "*HP Client Management Interface Software Providers*" (**HINWEIS:** Falls dieses Update noch nicht installiert sein sollte, können Sie die entsprechende Datei von der HP Website herunterladen und installieren.)
- Retail Point-of-Sale (RPOS)-Provider sind installiert. Dieses HP Update trägt die Bezeichnung "HP Retail Windows Management Instrumentation (WMI) Provider" (**HINWEIS:** Falls dieses Update noch nicht installiert sein sollte, können Sie die entsprechende Datei von der HP Website herunterladen und installieren.)

HINWEIS: Herunterladen und Installieren der CMI- und RPOS-Provider über die LANDesk Konsole
Wenn der CMI-Provider und der RPOS-Provider nicht bereits installiert sind, können Sie beide Provider remote über die LANDesk Konsole auf HP Geräten installieren. Verwenden Sie das Extra **Patch und Compliance** oder das Extra **Softwareverteilung** der LANDesk Management Suite.

Sie können jetzt das "verwaltete" HP Gerät scannen, das Geräteinventar anzeigen, Einstellungen für das BIOS und den TPM-Chip konfigurieren, HP Richtlinien erstellen und bereitstellen, HP Softwarerichtlinien mit der zugehörige HP Power Assistant-Einstellung erstellen und bereitstellen, die Extras HP Battery Check und HP Connection Manager verwenden u.s.w. Weitere Informationen finden Sie unter Verwalten von HP Geräten über die LANDesk Konsole.

HP Thin Client – Anforderungen

Folgende Anforderungen werden an HP-Thin Client-Geräte gestellt:

- Eines der folgenden Betriebssysteme ist auf dem Gerät installiert: Windows Embedded Standard 7 Enterprise (WES7), Windows Embedded Standard 09 Enterprise (WES09) oder HP ThinPro Ubuntu. (**WICHTIG**: HP ThinPro Ubuntu unterstützt gegenwärtig NUR den LANDesk Agenten für den Inventardienst.
- Standard LANDesk Agent ist installiert. Weitere Informationen finden Sie unter "Konfigurieren von HP Thin Client Windows Embedded Standard (WES)-Geräten" auf Seite 994 und "Konfigurieren von HP ThinPro Linux-Geräten" auf Seite 997.

Sind diese Voraussetzungen für HP Geräte erfüllt, können Sie einen der folgenden Schritte ausführen:

- Wenn Sie mit einem **LDMS 9.0-Coreserver** arbeiten, müssen Sie die HP Integrationssoftware installieren. Informationen hierzu finden Sie unter "Installieren der HP Hardware and Software Management-Software" auf Seite 990.
- Wenn Sie mit einem **LDMS 9.5-Coreserver** arbeiten, müssen Sie die HP Software nicht installieren. Jetzt haben Sie alle Vorbereitungen getroffen, um HP Clients und HP Thin Clients konfigurieren und über die LANDesk Konsole verwalten zu können. Weitere Informationen finden Sie unter "Konfigurieren von HP Geräten für LANDesk Verwaltungstasks" auf Seite 991.

Installieren der HP Hardware and Software Management-Software

Dieses Thema bietet schrittweise Anleitungen für die Installation von LANDesk Management Suite plus HP Hardware and Software Management auf Ihrem Coreserver.

WICHTIG: Die Installation ist NUR für einen LDMS 9.0-Coreserver bzw. in einer LDMS 9.0-Umgebung erforderlich
Dieses Verfahren ist nur dann anwendbar, wenn Sie LANDesk Management Suite Version 9.0 (mit installiertem SP3) ausführen. Wenn Sie LDMS 9.0 verwenden, müssen Sie die nachstehend

beschriebenen Schritte ausführen. Wenn Sie jedoch das Upgrade auf LANDesk Management Suite Version 9.5 vorgenommen haben, können Sie dieses Verfahren überspringen, denn alle HP Management-Extras sind standardmäßig in diese Version integriert.

Installieren der HP Management-Software auf Ihrem LDMS-Coreserver

WICHTIG: Einhaltung der Installationsanforderungen
Stellen Sie sicher, dass alle Anforderungen für die Installation erfüllt sind. Einzelheiten finden Sie unter "Installationsvoraussetzungen" auf Seite 989.

Führen Sie alle in der folgende Liste aufgeführten Schritte zur Installation der HP Software aus.

So installieren Sie die HP Software

1. Navigieren Sie auf dem Coreserver zur Seite LANDesk User Community DOC-24825 "How To Install LANDesk with HP Management" und laden Sie das Softwarepaket mit dem Namen "LD90-SP3-HP-Release-1.3.exe" herunter.
2. Führen Sie die heruntergeladene ausführbare Datei aus. Sie wird in folgendes Verzeichnis extrahiert: C:\LD90-HP (Sie können aber auch ein anderes Verzeichnis wählen.)
3. Öffnen Sie das extrahierte Verzeichnis.
4. Öffnen Sie das Verzeichnis "LD90-SP3-HP-Release-1.3".
5. Extrahieren Sie die Datei "LD90-SP3-HP-Release-1.3.zip".
6. Öffnen Sie das extrahierte Verzeichnis.
7. Führen Sie das Programm Setup.exe aus.
8. Folgen Sie den Anweisungen.
9. Klicken Sie auf der Seite "Installieren" auf **Installieren**. Der Installations-Assistent gibt Aufschluss über den Fortschritt und den Status der Installation.
10. Klicken Sie auf der Seite "Abgeschlossen" auf **Fertig stellen**.
11. Wenn die Nachricht "Abgeschlossen / Installation erfolgreich" angezeigt wird, klicken Sie auf **Schließen**.

Wie geht´s weiter?

Im nächsten Schritt müssen Sie Ihre HP Geräte mit dem Standard LANDesk Agenten konfigurieren. Weitere Informationen finden Sie unter "Konfigurieren von HP Geräten für LANDesk Verwaltungstasks" auf Seite 991.

Konfigurieren von HP Geräten für LANDesk Verwaltungstasks

Bevor Sie Ihre HP Geräte verwalten können, müssen Sie diese mit dem Standard LANDesk Agenten (CBA oder Common Base Agent) konfigurieren. Hierdurch werden die Geräte zu verwalteten Geräten in der LANDesk Coredatenbank und Sie können die verschiedenen Verwaltungstasks – einschließlich spezifischer, integrierter HP Hardware and Software Management-Tasks – über die LANDesk Konsole ausführen.

Zusätzliche HP Geräte, die konfiguriert werden können

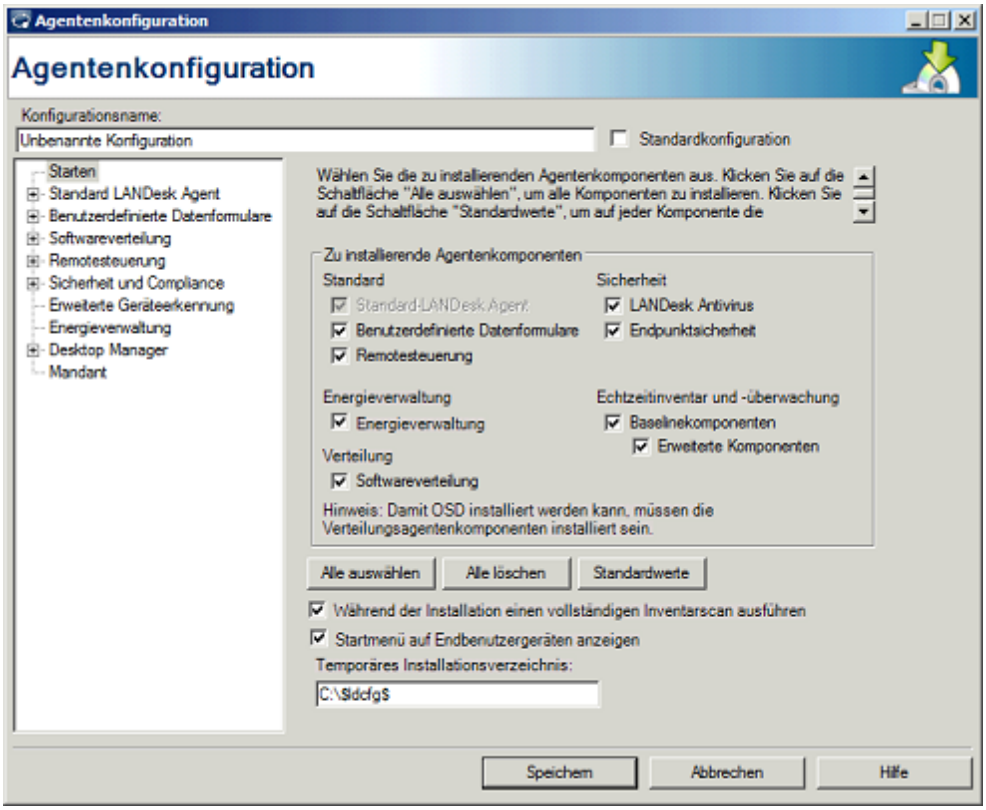
Sie können darüber hinaus die folgenden Typen von HP Plattformen (als verwaltete Geräte) konfigurieren und mit den LANDesk Extras verwalten:

- Windows Embedded Standard 7 Enterprise (WES7): Weitere Informationen finden Sie unter "Konfigurieren von HP Thin Client Windows Embedded Standard (WES)-Geräten" auf Seite 994.
- Windows Embedded Standard 09 Enterprise (WES09): Weitere Informationen finden Sie unter "Konfigurieren von HP Thin Client Windows Embedded Standard (WES)-Geräten" auf Seite 994.
- HP ThinPro Linux Ubuntu: Weitere Informationen finden Sie unter "Konfigurieren von HP ThinPro Linux-Geräten" auf Seite 997.

Bereitstellen des LANDesk Agenten für HP Geräte

So stellen Sie den LANDesk Agenten bereit

1. Ordnen Sie dem Coreserver auf dem HP Computer ein Laufwerk zu, steuern Sie den Ordner LDLogon an und führen Sie wscfg32.exe aus. (Oder stellen Sie eine Agentenkonfiguration von der Konsole aus über einen geplanten Task bereit, indem Sie das Dialogfeld "Agentenkonfiguration" über **Extras > Konfiguration > Agentenkonfiguration** aufrufen.)
2. Klicken Sie mit der rechten Maustaste auf **Eigene Konfiguration** und klicken Sie dann auf **Neue Windows-Agentenkonfiguration**.
3. Geben Sie auf der Seite **Start** einen eindeutigen Namen für diese Konfiguration ein.
4. Vergewissern Sie sich auf der **Start**seite, dass unter **Echtzeitinventar und -überwachung** sowohl die Option **Baselinekomponenten** als auch die Option **Erweiterte Komponenten** markiert sind. (**HINWEIS:** Die LANDesk Alarmierungsfunktion wird standardmäßig mit dem Standard LANDesk Agenten aktiviert.)



5. Wählen Sie die einzelne Seiten aus und geben Sie die Optionen an, die Sie für diese Konfiguration übernehmen möchten und die dann für Zielgeräte bereitgestellt werden sollen. (Wenn Sie nähere Informationen wünschen, klicken Sie auf der betreffenden Seite auf **Hilfe**.)
6. Klicken Sie auf **Installieren**.

   ODER

   Wenn Sie die Agentenkonfiguration *von der LANDesk Konsole aus* für Zielgeräte bereitstellen, klicken Sie auf **Speichern**, um den Task zum Fenster des Extras "Geplante Tasks" hinzuzufügen. Dort können Sie dann einen Task zur Bereitstellung der Agentenkonfiguration für die von Ihnen gewünschten HP Zielgeräte konfigurieren.

Bringen Sie Ihre HP Geräte mit der LANDesk Management Suite unter Ihre Kontrolle

Sobald ein HP Gerät mit dem LANDesk Agenten konfiguriert wurde, wird es zu einem "verwalteten" Gerät in der LANDesk Netzwerkumgebung.

In der Netzwerkansicht

In der Netzwerkansicht der LANDesk Konsole können Sie mit der rechten Maustaste auf ein verwaltetes HP Gerät klicken und das Kontextmenü öffnen, das Ihnen folgende Funktionen bietet:

- Ausführen eines Inventarscans
- Anzeigen der Inventardaten des HP Geräts (BIOS-Einstellungen, TPM Sicherheitschip-Einstellungen, Daten zu HP Power Assistant, HP Battery Check, HP Connection Manager sowie zu RPOS-Peripheriegeräten)

In der Konsole

Die Konsole bieten Ihnen ferner folgende Funktionen:

- Zugriff auf die neuen integrierten HP Hardware Management-Extras in der LANDesk Konsole
- Konfigurieren (Ändern/Aktualisieren) von HP BIOS-Einstellungen und HP TPM-Chipeinstellungen
- Konfigurieren (Ändern/Aktualisieren) von HP Power Assistant-Einstellungen
- Erstellen und Ausführen von Abfragen auf der Basis von HP gerätespezifischen Inventardaten (Komponenten und Attribute)
- Konfigurieren von Alarmen auf der Basis von HP Geräteinventardaten
- Generieren von Berichten auf der Basis von HP Geräteinventardaten

Ausführliche Informationen und schrittweise Anleitungen zu allen diesen Tasks finden Sie unter Verwalten von HP Geräten über die LANDesk Konsole.

Verwandte Themen

Verwalten von HP-Geräten über die LANDesk Konsole.

Konfigurieren von HP Thin Client Windows Embedded Standard (WES)-Geräten

Bevor Sie Ihre HP Thin Client-Geräte verwalten können, müssen Sie diese mit dem Standard LANDesk Agenten (CBA oder Common Base Agent) konfigurieren. Hierdurch werden die Geräte zu verwalteten Geräten in der LANDesk Coredatenbank und Sie können die verschiedenen Verwaltungstasks – einschließlich LANDesk Partner HP Hardware and Software Management-Tasks – über die LANDesk Konsole ausführen.

LANDesk Management Suite Version 9.5 bietet Unterstützung für die folgenden HP Thin Client-WES-Plattformen:

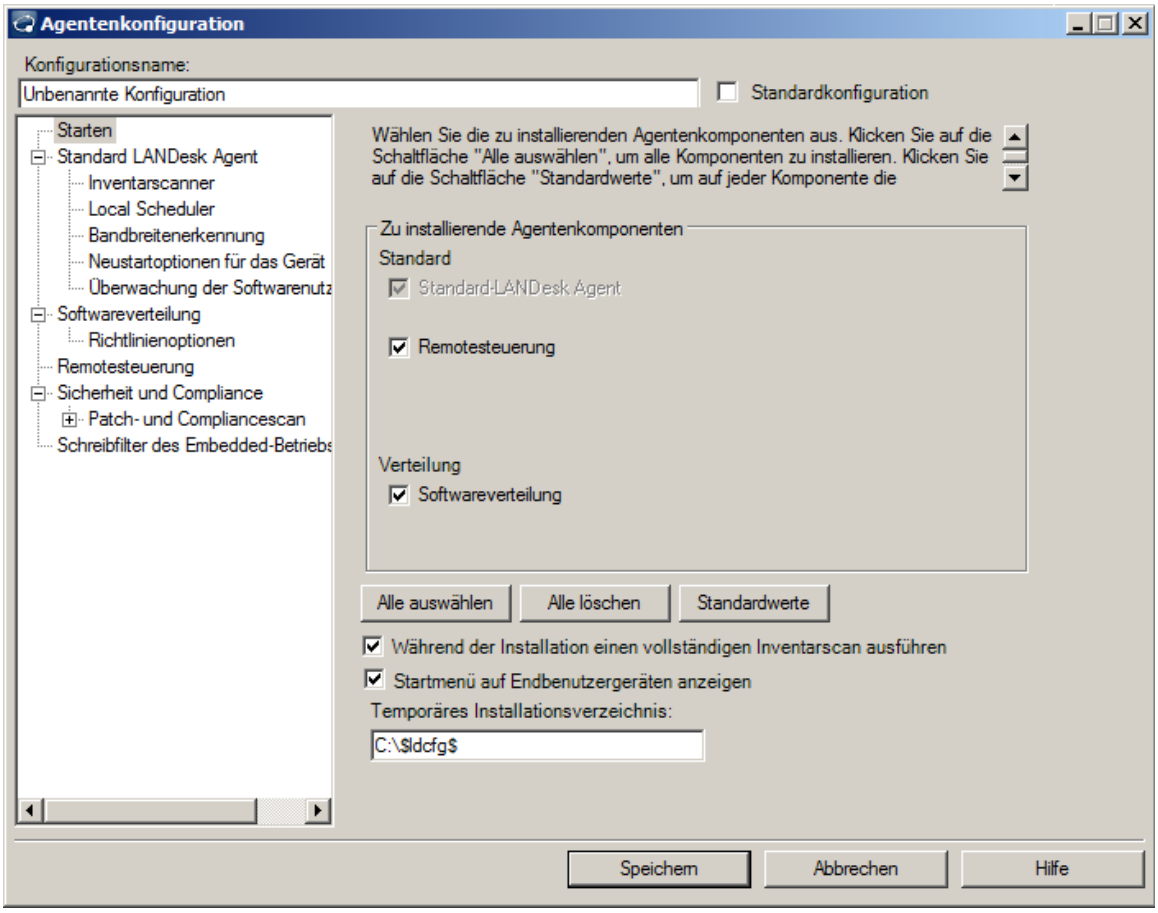
- Windows Embedded Standard 7 Enterprise (WES7)
- Windows Embedded Standard 09 Enterprise (WES09)

Bereitstellen des LANDesk Agenten für HP Thin Client-WES-Geräte

So stellen Sie den LANDesk Agenten bereit

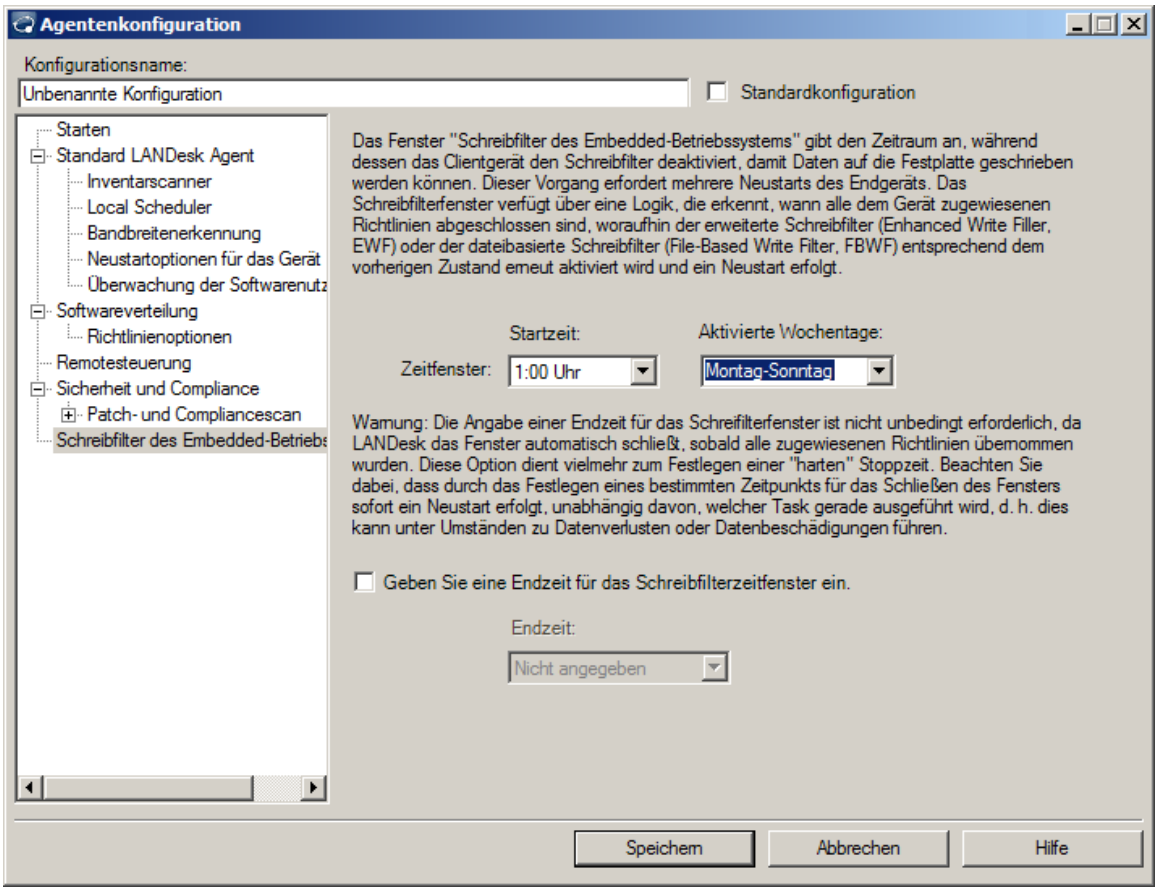
1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**, um das Dialogfeld "Agentenkonfiguration" zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf **Eigene Konfiguration** und klicken Sie dann auf **Neue Windows Embedded Standard-Agentenkonfiguration**.
3. Geben Sie auf der Seite **Start** einen eindeutigen Namen für diese Konfiguration ein.

4. Das Dialogfeld für die Agentenkonfiguration weist ähnliche Optionen und Steuerelemente auf wie die Standard-Windows-Agentenkonfiguration. Wählen Sie die einzelne Seiten aus und geben Sie die Optionen an, die Sie für diese Konfiguration übernehmen möchten und die dann für Zielgeräte bereitgestellt werden sollen. (Wenn Sie nähere Informationen wünschen, klicken Sie auf der betreffenden Seite auf **Hilfe**.)



5. Ein spezifisches Feature des HP Thin Client-WES-Managements ist die Schreibfilteroption für Embedded-Betriebssysteme. Klicken Sie auf die Seite **Schreibfilter des Embedded-Betriebssystems**, um einen Zeitraum zu definieren, während dem der Schreibfilter auf dem verwalteten Gerät deaktiviert wird, damit ein LANDesk Administrator Wartungsaufgaben auf dem Gerät ausführen kann. (**HINWEIS:** Hierbei wird der Schreibfilter auf der Festplatte des Zielgeräts deaktiviert, das Gerät wird neu gestartet und am Ende des definierten Zeitraums bzw. sobald alle geplanten Tasks und Prozesse abgeschlossen sind, wird der Schreibfilter wieder eingeschaltet und das Gerät nochmals neu gestartet.) Sie können eine Startzeit angeben und die Wochentage, an denen Wartungszeitfenster zulässig sind, sowie eine zwingende Endzeit.

   Weitere Informationen hierzu finden Sie unter "Bereitstellen des Schreibfilters für Windows Embedded-Standardgeräte" auf Seite 141.


Agentenkonfiguration
Konfigurationsname:
Unbenannte Konfiguration
Standardkonfiguration
Starten
Standard LANDesk Agent
Inventarscanner
Local Scheduler
Bandbreitenerkennung
Neustartoptionen für das Gerät
Überwachung der Softwarenutz
Softwareverteilung
Richtlinienoptionen
Remotesteuerung
Sicherheit und Compliance
Patch- und Compliancescan
Schreibfilter des Embedded-Betriebs
Das Fenster "Schreibfilter des Embedded-Betriebssystems" gibt den Zeitraum an, während dessen das Clientgerät den Schreibfilter deaktiviert, damit Daten auf die Festplatte geschrieben werden können. Dieser Vorgang erfordert mehrere Neustarts des Endgeräts. Das Schreibfilterfenster verfügt über eine Logik, die erkennt, wann alle dem Gerät zugewiesenen Richtlinien abgeschlossen sind, woraufhin der erweiterte Schreibfilter (Enhanced Write Filter, EWF) oder der dateibasierte Schreibfilter (File-Based Write Filter, FBWF) entsprechend dem vorherigen Zustand erneut aktiviert wird und ein Neustart erfolgt.
Startzeit:
Aktivierte Wochentage:
Zeitfenster:
1:00 Uhr
Montag-Sonntag
Warnung: Die Angabe einer Endzeit für das Schreifilterfenster ist nicht unbedingt erforderlich, da LANDesk das Fenster automatisch schließt, sobald alle zugewiesenen Richtlinien übernommen wurden. Diese Option dient vielmehr zum Festlegen einer "harten" Stoppzeit. Beachten Sie dabei, dass durch das Festlegen eines bestimmten Zeitpunkts für das Schließen des Fensters sofort ein Neustart erfolgt, unabhängig davon, welcher Task gerade ausgeführt wird, d. h. dies kann unter Umständen zu Datenverlusten oder Datenbeschädigungen führen.
Geben Sie eine Endzeit für das Schreibfilterzeitfenster ein.
Endzeit:
Nicht angegeben
Speichern
Abbrechen
Hilfe

VORSICHT: Wenn Sie eine bestimmte Endzeit für die Aktivierung des Schreibfilters und die Ausführung von Richtlinien und Prozessen definieren, denken Sie daran, dass es zu einem Verlust oder zur Beschädigung von Daten kommen kann, wenn beim Erreichen der Endzeit nicht alle Prozesse abgeschlossen werden konnten. Sie müssen daher den Zeitbedarf für die Durchführung und den Abschluss aller angewendeten Richtlinien und Task genau bestimmen und festlegen. Oder aber Sie definieren KEINE Endzeit.

6. Klicken Sie auf **Speichern**. Damit wird der Task zum Fenster des Extras "Geplante Tasks" hinzugefügt. Dort können Sie einen Task zur Bereitstellung der Agentenkonfiguration auf Ihren HP Thin Client-WES-Zielgeräten konfigurieren.

Verwandte Themen

"Verwalten von HP Thin Client-Geräten über die LANDesk Konsole" auf Seite 1028

Konfigurieren von HP ThinPro Linux-Geräten

Bevor Sie Ihre HP ThinPro Linux-Geräte verwalten können, müssen Sie diese mit dem Standard LANDesk Agenten (CBA oder Common Base Agent) konfigurieren. Hierdurch werden die Geräte zu verwalteten Geräten in der LANDesk Coredatenbank und Sie können die verschiedenen Verwaltungstasks – einschließlich LANDesk Partner HP Hardware and Software Management-Tasks – über die LANDesk Konsole ausführen.

LANDesk Management Suite Version 9.5 bietet Unterstützung für die folgenden HP ThinPro Linux-Plattformen:

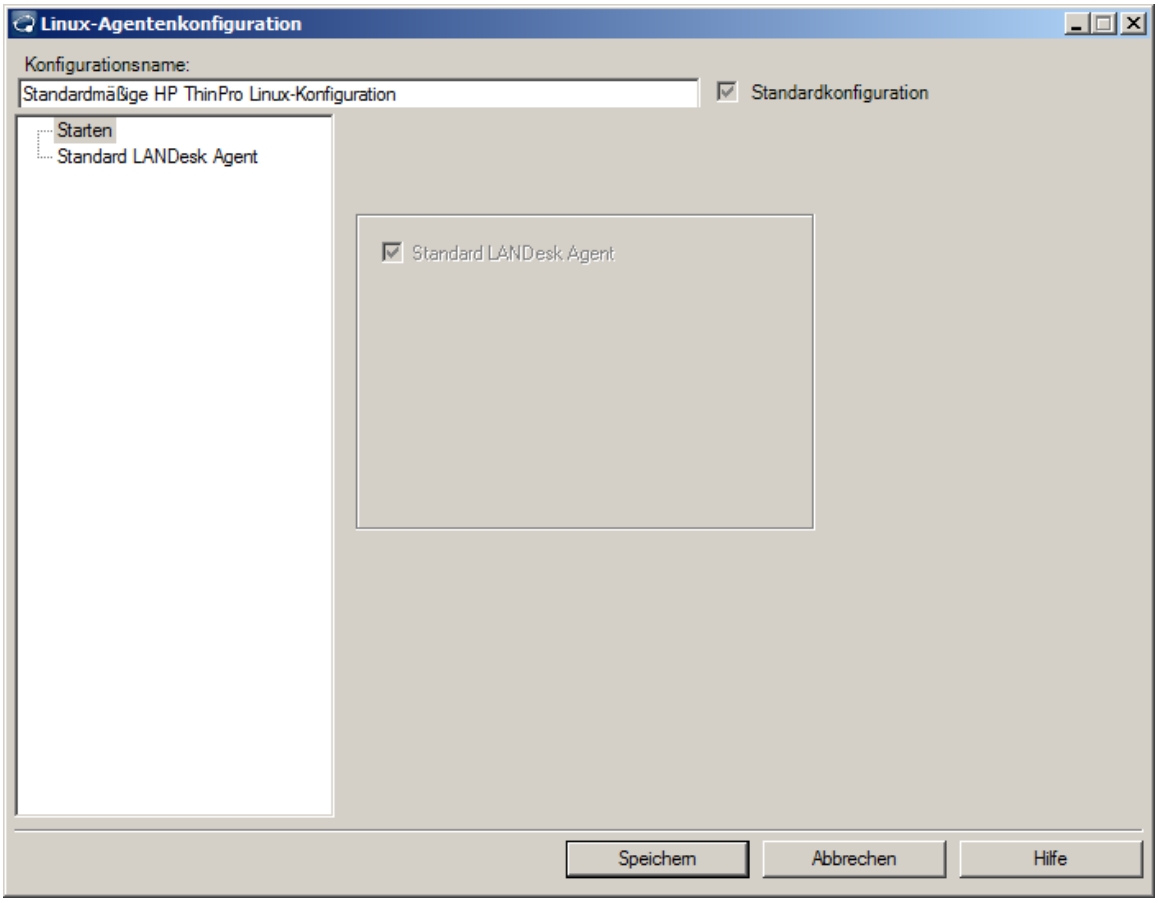
- HP ThinPro Linux Ubuntu

Bereitstellen des LANDesk Agenten für HP ThinPro Linux-Geräte

So stellen Sie den LANDesk Agenten bereit

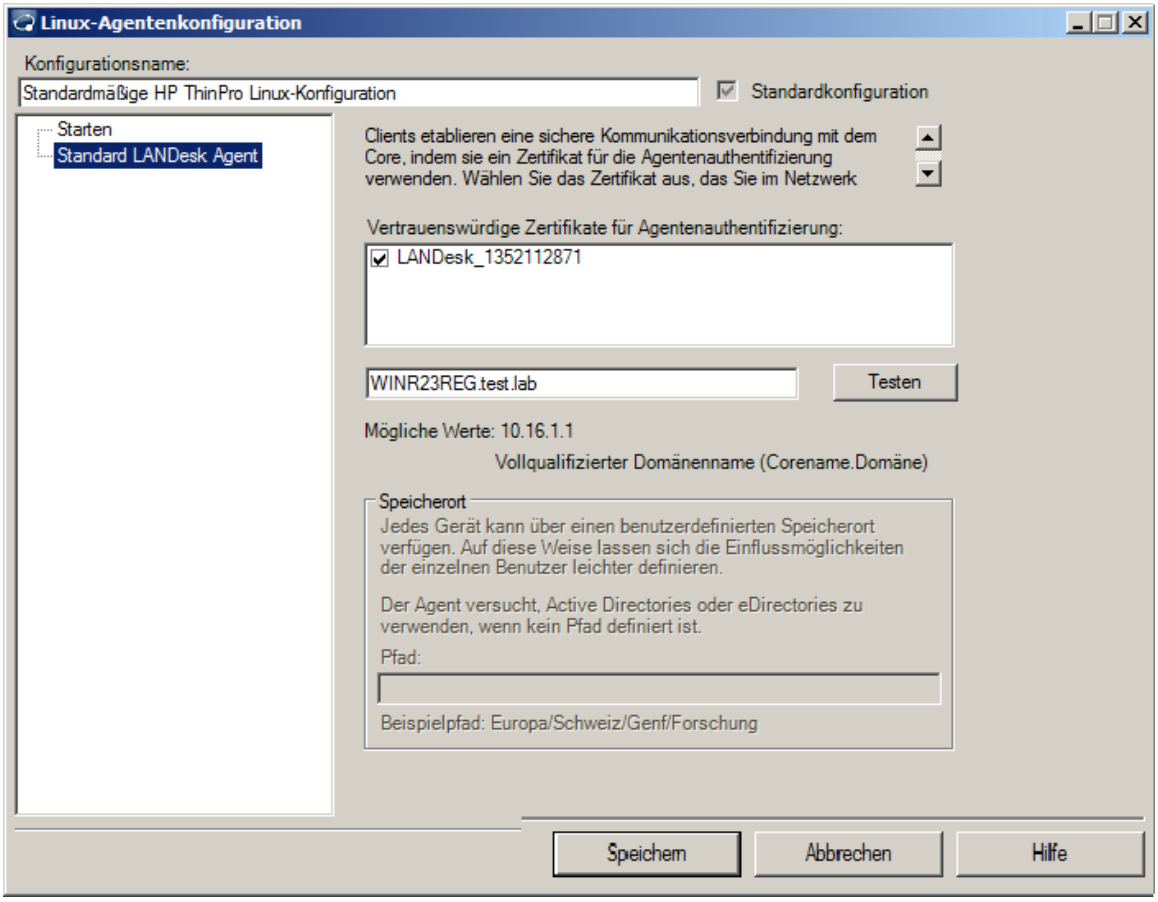
1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Agentenkonfiguration**, um das Dialogfeld "Agentenkonfiguration" zu öffnen.
2. Klicken Sie mit der rechten Maustaste auf **Eigene Konfiguration** und klicken Sie dann auf **Neue HP ThinPro Linux-Agentenkonfiguration**.

3. Das Dialogfeld "HP ThinPro Linux-Agentenkonfiguration" stellt eine reduzierte Version der Windows Agentenkonfiguration dar. Es umfasst die Seite "Standard LANDesk Agent".



4. Geben Sie auf der Seite **Start** einen eindeutigen Namen für diese Konfiguration ein.

5. Klicken Sie auf die Seite **Standard LANDesk Agent** und geben Sie Ihre Einstellungen an. (Detaillierte Informationen erhalten Sie, wenn Sie auf Hilfe klicken.)


Linux-Agentenkonfiguration
Konfigurationsname:
Standardmäßige HP ThinPro Linux-Konfiguration
Standardkonfiguration
Starten
Standard LANDesk Agent
Clients etablieren eine sichere Kommunikationsverbindung mit dem Core, indem sie ein Zertifikat für die Agentenauthentifizierung verwenden. Wählen Sie das Zertifikat aus, das Sie im Netzwerk
Vertrauenswürdige Zertifikate für Agentenauthentifizierung:
LANDesk_1352112871
WINR23REG.test.lab
Testen
Mögliche Werte: 10.16.1.1
Vollqualifizierter Domänenname (Corename.Domäne)
Speicherort
Jedes Gerät kann über einen benutzerdefinierten Speicherort verfügen. Auf diese Weise lassen sich die Einflussmöglichkeiten der einzelnen Benutzer leichter definieren.
Der Agent versucht, Active Directories oder eDirectories zu verwenden, wenn kein Pfad definiert ist.
Pfad:
Beispielpfad: Europa/Schweiz/Genf/Forschung
Speichern
Abbrechen
Hilfe

6. Klicken Sie auf **Speichern**. Damit wird der Task zum Fenster des Extras "Geplante Tasks" hinzugefügt. Dort können Sie einen Task zur Bereitstellung der Agentenkonfiguration auf Ihren HP ThinPro Linux-Zielgeräten konfigurieren.

Verwandte Themen

"Verwalten von HP Thin Client-Geräten über die LANDesk Konsole" auf Seite 1028

Zugriff auf die integrierten HP Extras in der LANDesk Konsole

Sie können sich jetzt bei der LANDesk Konsole anmelden und auf die integrierten HP Hardware Management-Extras zugreifen, die bei der Installation der Software "LANDesk Management Suite plus HP Hardware and Software Management" zur LANDesk Konsole hinzugefügt werden.

Von der Konsole aus haben Sie außerdem Zugriff auf die verwalteten HP Geräteinventarkomponenten wie auch die Retail Point-of-Sale (RPOS)-Peripheriegeräte.

LANDesk plus HP Management fügt zwei neue HP spezifische Extras zum Menü **Konfigurieren** der Konsole hinzu:

- **HP BIOS-Konfiguration**
- **HP TPM-Konfiguration**

Ferner wird ein neues HP spezifisches Extra zum Extra-Fenster "Sicherheitskonfigurationen" hinzugefügt.

- **HP Softwarerichtlinien**

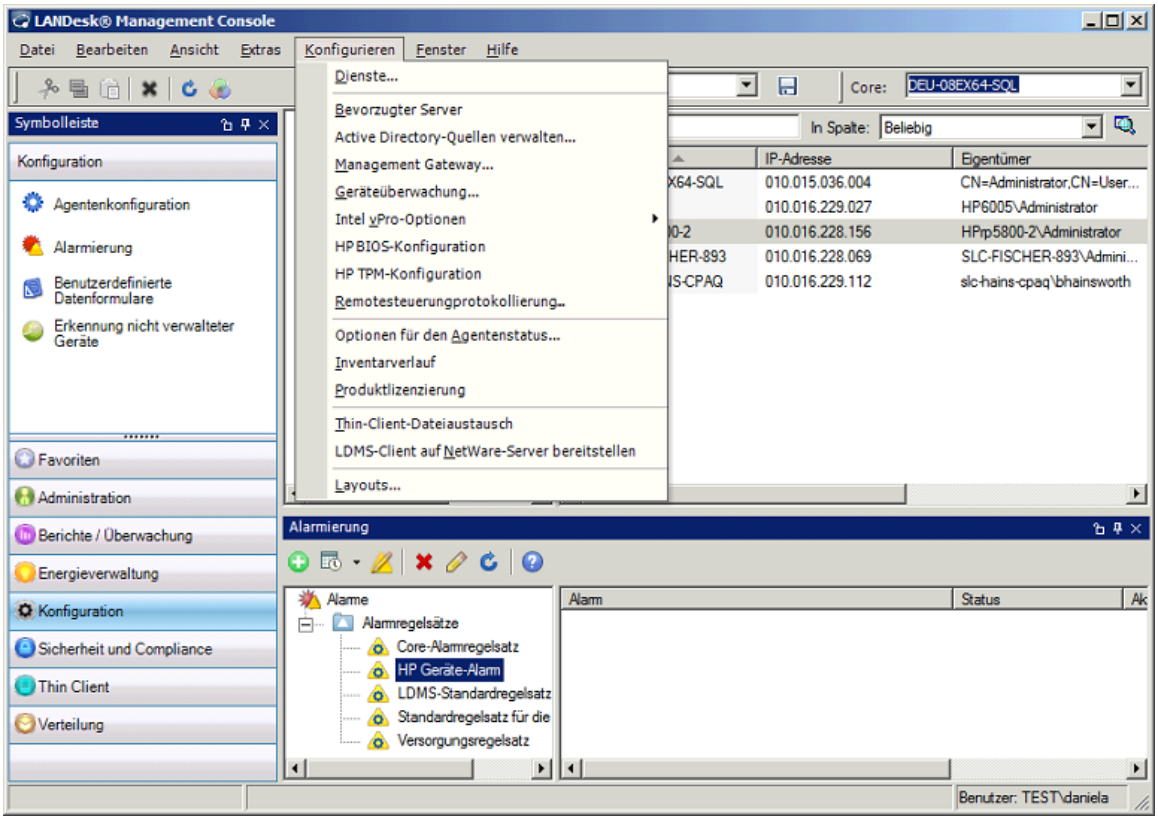
Beschreibungen dieser integrierten HP Extras finden Sie in der "Hilfe zur Konfiguration der BIOS-Einstellungen" auf Seite 1028, "Hilfe zur TPM-Konfiguration" auf Seite 1029 und der "Hilfe zu den HP Softwarerichtlinien-Einstellungen" auf Seite 1030.

WICHTIG: Starten Sie die Konsole neu, damit die HP Extras angezeigt werden
Sie MÜSSEN die LANDesk Konsole (sowie alle anderen zusätzlichen Konsolen in Ihrem LANDesk System) schließen und neu starten, damit die neuen HP Extras im Menü **Konfigurieren** angezeigt werden.

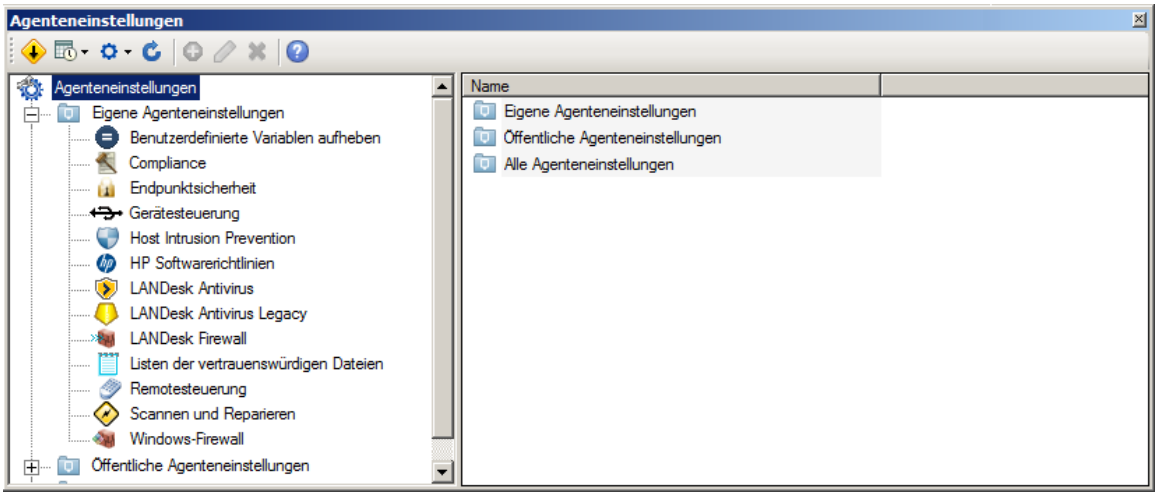
WICHTIG: LANDesk Administratorrechte erforderlich
Nur Benutzer mit dem Recht eines LANDesk Administrators können die HP Extras sehen und verwenden.

So greifen Sie auf die HP Management-Extras zu

1. Wählen Sie in der Konsole in der **Netzwerkansicht** das verwaltetes HP Gerät aus.
2. Klicken Sie auf das Extra-Menü **Konfigurieren** und anschließend auf das Extra **HP Konfiguration** in der Liste, die Sie öffnen möchten.



3. Beim neuen Extra "HP Softwarerichtlinien" klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Sicherheitskonfigurationen**, öffnen Sie den Knoten **Eigene Sicherheitskonfigurationen** und klicken Sie auf **HP Softwarerichtlinien**.



Ausführen eines Inventarscans und Anzeigen des HP Geräteinventars

Sobald Sie den LANDesk Inventarscanner auf einem verwalteten HP Gerät ausgeführt haben, können Sie dessen Inventardaten in der LANDesk Konsole anzeigen.

In einer Geräteinventaransicht finden Sie die folgenden Hardware- und Softwarekomponentendaten:

- Daten zu BIOS-Einstellungen
- HP Power Assistant-Daten
- HP Battery Check-Daten
- HP Connection Manager-Daten

Sie können ferner das Inventar für die verknüpften HP Retail Point-of-Sale (RPOS)-Geräte anzeigen.

HINWEIS: Geräteinventardaten
Die Inventardaten für gescannte Geräte werden in der LANDesk Coredatenbank gespeichert. Sie können dann mit verschiedenen Extras über die LANDesk Konsole angezeigt und genutzt werden, beispielsweise über die Inventaransicht, in Berichten, benutzerdefinierten Abfragen, für Alarme usw.

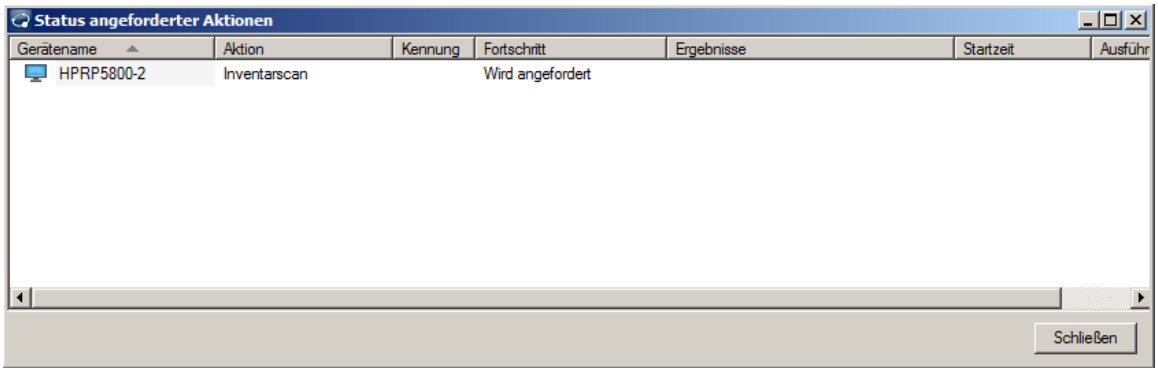
Ausführen eines Inventarscans auf einem verwalteten Gerät

Mit diesem Vorgang werden Informationen zu den Hardware- und Softwarekomponenten von verwalteten Geräten gesammelt und in der LANDesk Coredatenbank gespeichert.

So führen Sie einen Inventarscan aus

1. Klicken Sie in der Konsole mit der rechten Maustaste auf ein verwaltetes HP Gerät, um auf dessen Kontextmenü zuzugreifen.
2. Klicken Sie auf **Inventarscan** und wählen Sie den Scantyp aus, den Sie ausführen möchten.

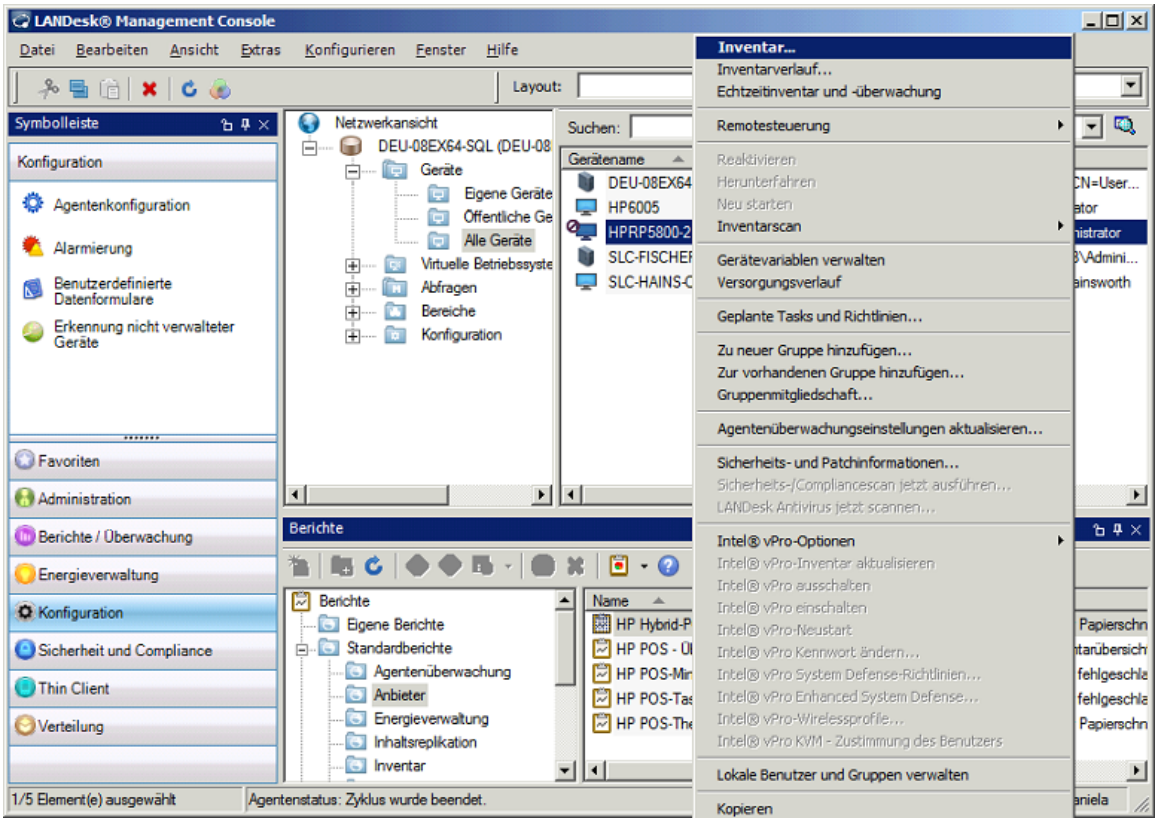
3. Im **Status**fenster werden der Fortschritt und andere Details zur angeforderten Aktion angezeigt.



Anzeigen des Inventars eines verwaltetes HP Geräts

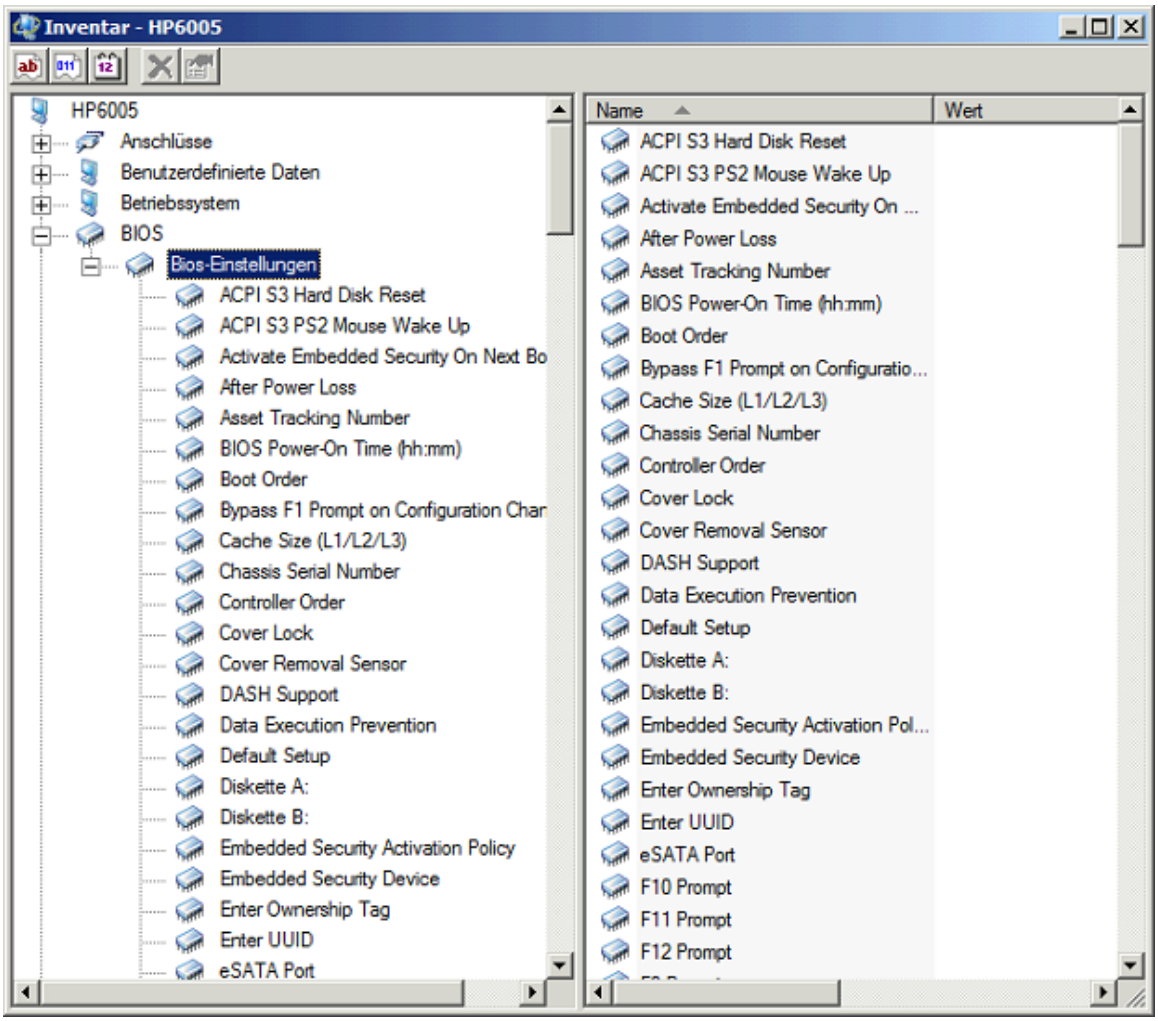
So zeigen Sie das Inventars eines verwaltetes HP Geräts an

1. Klicken Sie in der Konsole mit der rechten Maustaste auf ein verwaltetes HP Gerät, um dessen Kontextmenü zu öffnen, und klicken Sie dann auf **Inventar**.

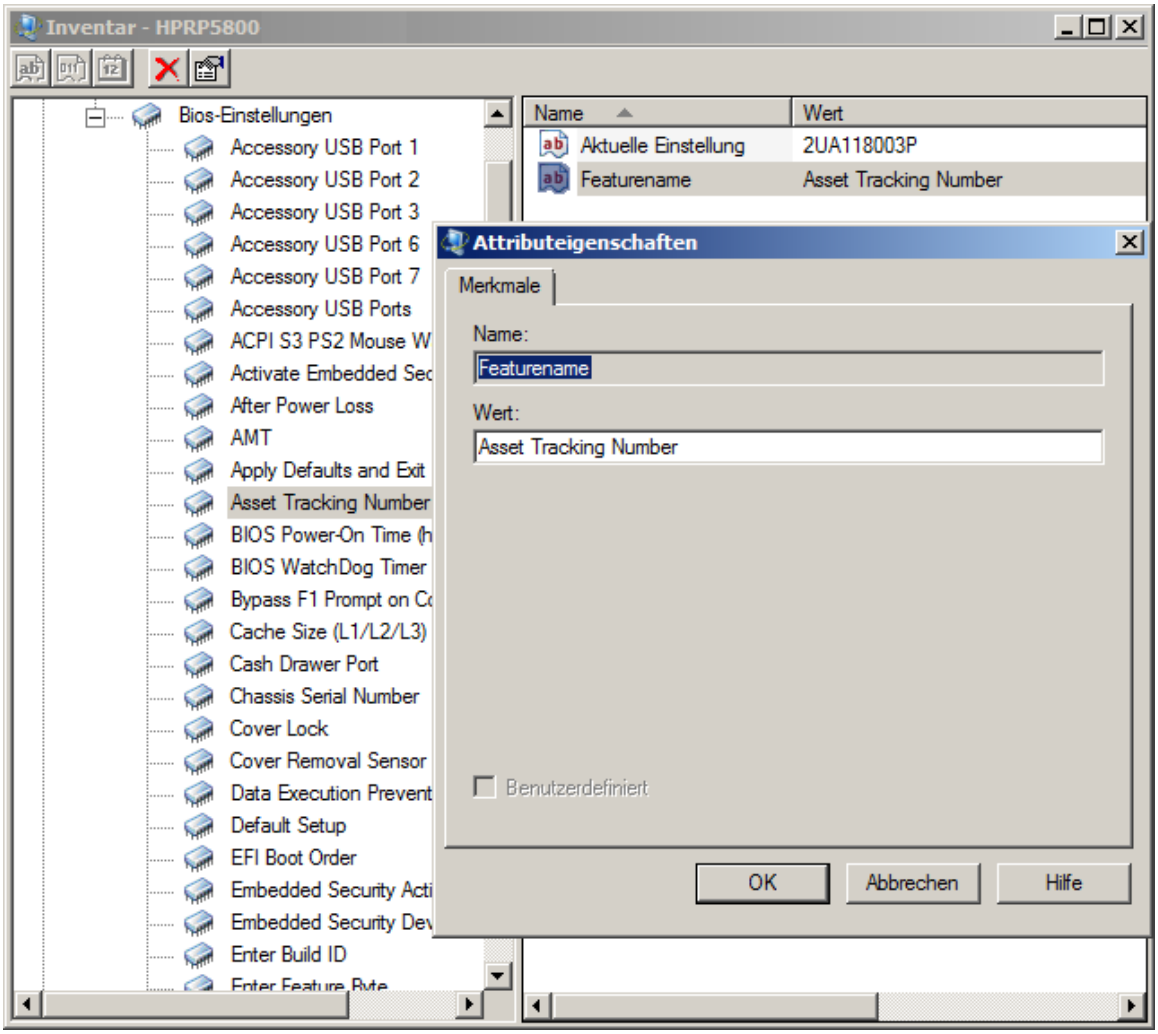


2. Im Fenster **Inventar** können Sie auswählen, welche Art von gescannten HP Daten Sie einsehen möchten. Wenn Sie beispielsweise die Daten zu den BIOS-Einstellungen des HP Geräts sehen möchten, öffnen Sie die **BIOS**-Komponente

und anschließend den Knoten **BIOS-Einstellungen**.



3. Um die Eigenschaften eines bestimmten Attributs anzuzeigen, wählen Sie das gewünschte Attribut in der Liste aus und doppelklicken Sie auf eine Eigenschaft im rechten Fensterausschnitt.

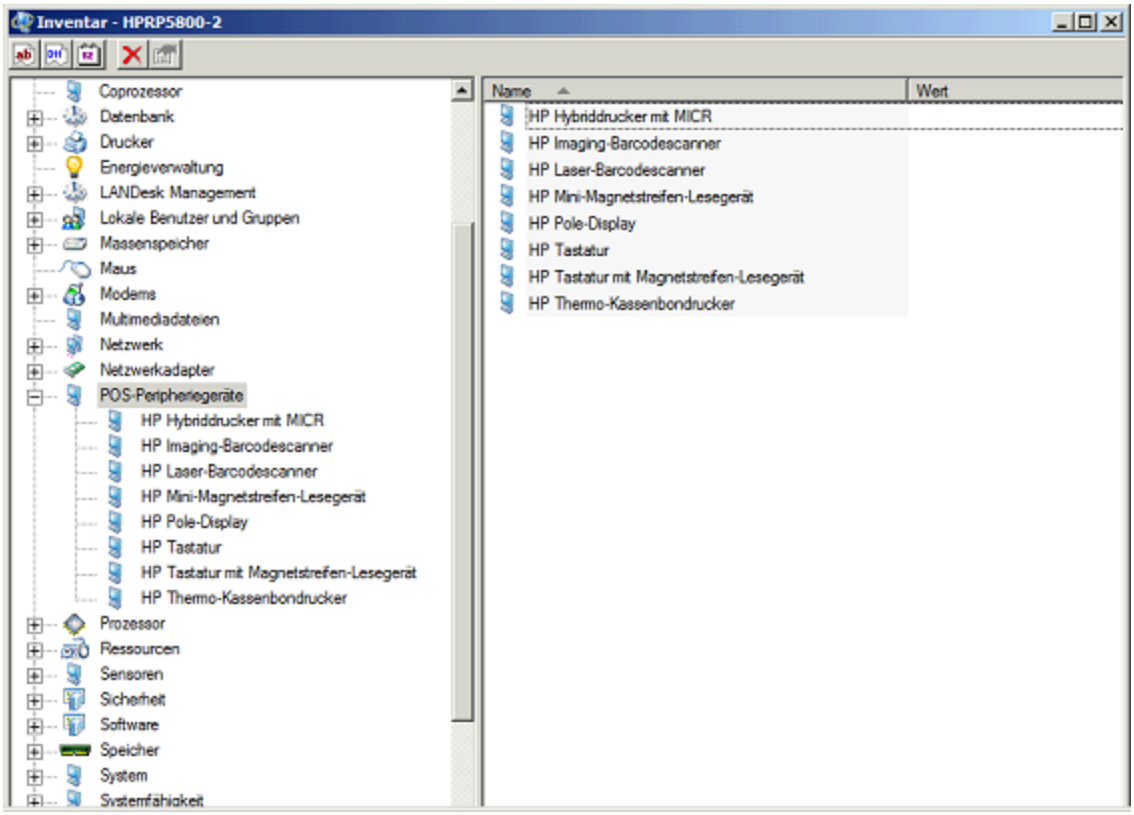


4. Klicken Sie auf **OK**, um das Dialogfeld "Eigenschaften" zu schließen.
5. Sie können auch den Knoten **Hewlett-Packard** öffnen, um zusätzliche HP spezifische Daten anzuzeigen, wie zum Beispiel: Daten für HP Power Assistant, HP Battery Check und HP Connection Manager. Weitere Informationen finden Sie unter "Verwenden von HP Power Assistant" auf Seite 1011, "Verwenden von HP Battery Check" auf Seite 1013 und "Verwenden von HP Connection Manager" auf Seite 1014.

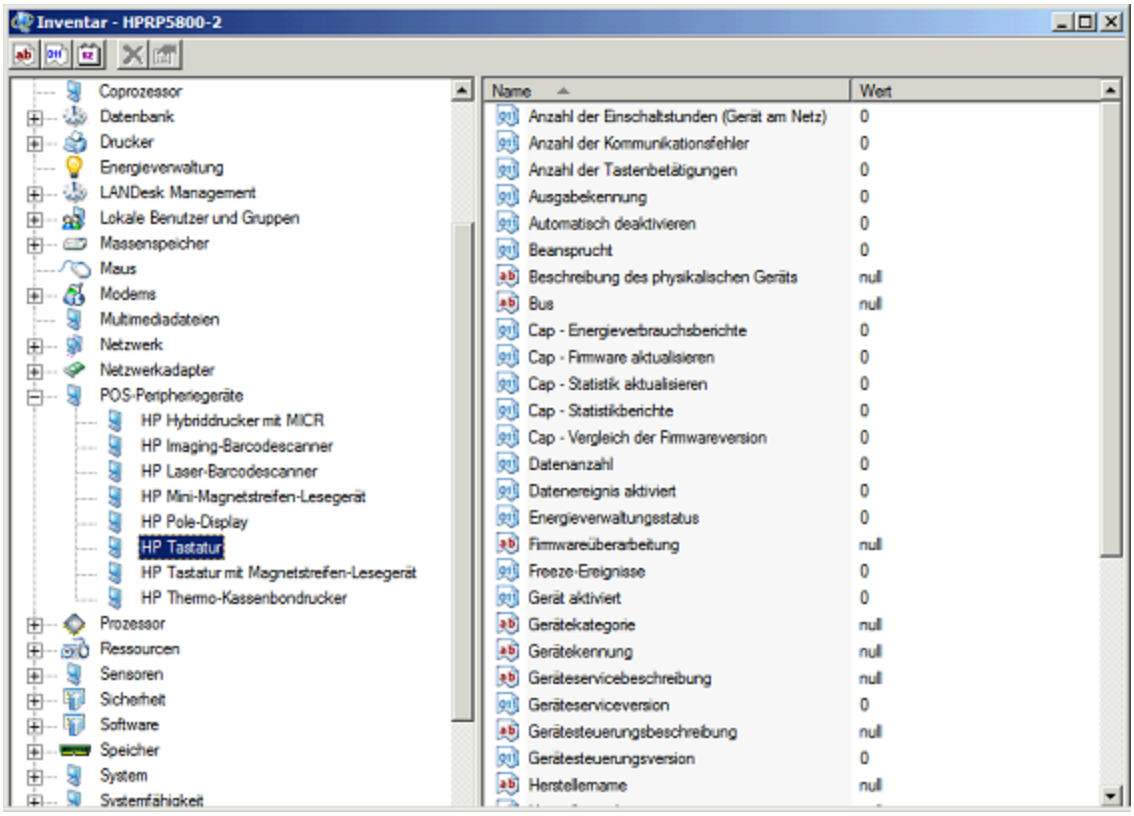
Anzeigen des Inventars eines HP Retail POS (RPOS)-Peripheriegeräts

So zeigen Sie das Inventar eines HP Retail POS (RPOS)-Peripheriegeräts an

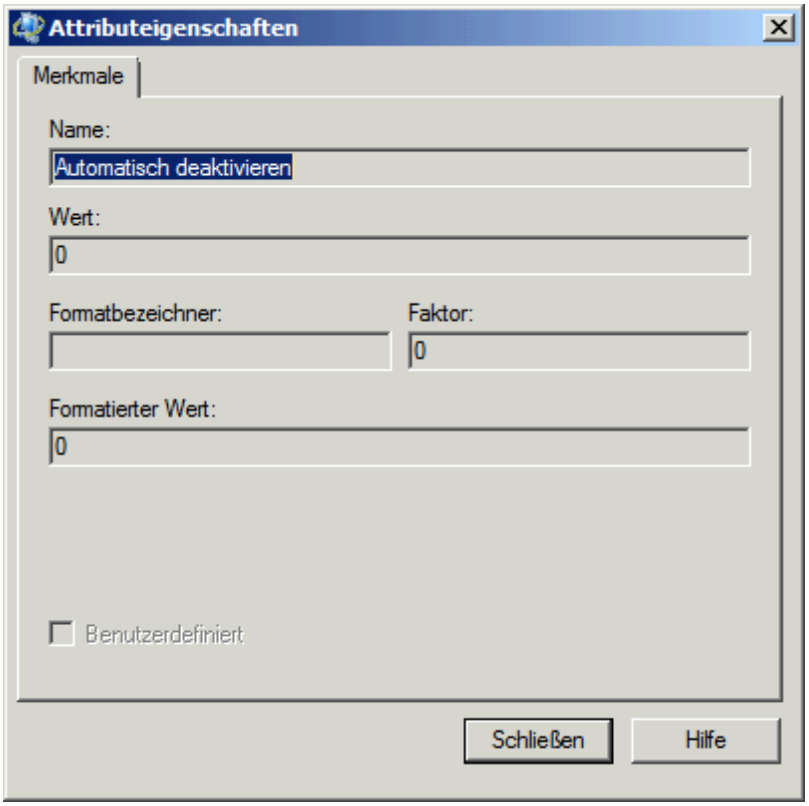
1. Klicken Sie in der Konsole mit der rechten Maustaste auf ein HP Gerät und klicken Sie dann auf **Inventar > POS-Peripheriegeräte**.


Inventar - HPRP5800-2
Coprozessor
Datenbank
Drucker
Energieverwaltung
LANDesk Management
Lokale Benutzer und Gruppen
Massenspeicher
Maus
Modems
Multimediadateien
Netzwerk
Netzwerkadapter
POS-Peripheriegeräte
HP Hybriddrucker mit MICR
HP Imaging-Barcodescanner
HP Laser-Barcodescanner
HP Mini-Magnetstreifen-Lesegerät
HP Pole-Display
HP Tastatur
HP Tastatur mit Magnetstreifen-Lesegerät
HP Thermo-Kassenbondrucker
Prozessor
Ressourcen
Sensoren
Sicherheit
Software
Speicher
System
Systemfähigkeit
Name
Wert
HP Hybriddrucker mit MICR
HP Imaging-Barcodescanner
HP Laser-Barcodescanner
HP Mini-Magnetstreifen-Lesegerät
HP Pole-Display
HP Tastatur
HP Tastatur mit Magnetstreifen-Lesegerät
HP Thermo-Kassenbondrucker

2. Um die Inventarattribute und -werte eines bestimmten RPOS-Geräts anzuzeigen, wählen Sie das Gerät (zum Beispiel: **HP Tastatur**) aus.



3. Um die Eigenschaften eines bestimmten Attributs anzuzeigen, doppelklicken Sie auf den Attributnamen (zum Beispiel: **Automatisch deaktivieren**).



WICHTIG: Wie LANDesk Management Suite HP Gerätedaten sammelt und speichert
Der LANDesk Coreserver führt eine proprietäres Dienstprogramm (die ausführbare Datei LDHPMgr.exe) aus. Diese sammelt spezifische Daten von den verwalteten HP Geräten in Ihrem Netzwerk. Diese Informationen werden dann von einem weiteren Dienstprogramm (der ausführbare Datei HPScanner.exe) in die LANDesk Coredatenbank geschrieben.

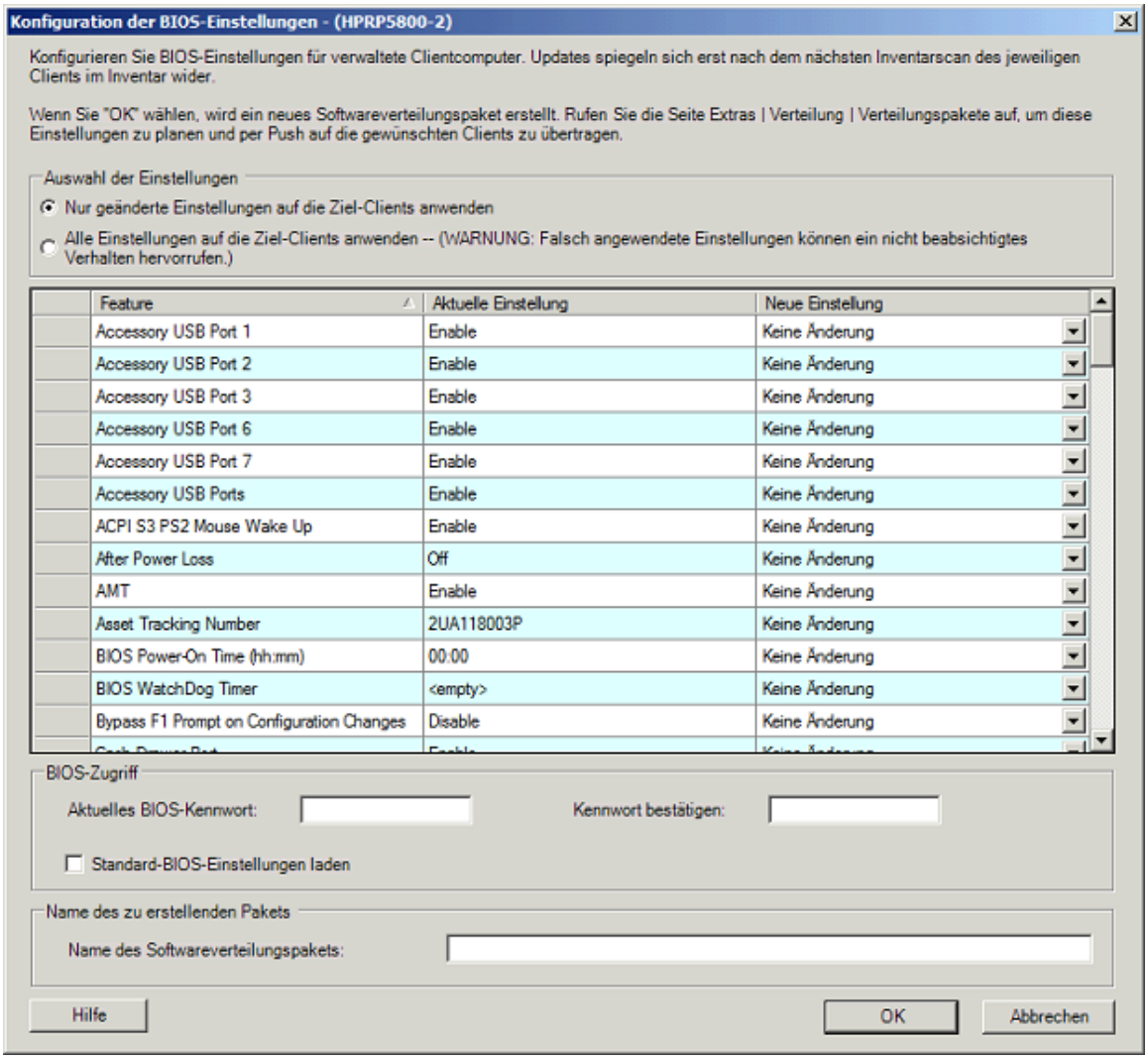
Erstellen und Bereitstellen von HP BIOS-Einstellungen für HP Zielgeräte

Wenn Sie die BIOS-Einstellungen auf einem oder mehreren der von Ihnen verwalteten HP Geräte remote ändern möchten, konfigurieren Sie die BIOS-Einstellungen in der LANDesk Konsole und stellen diese dann für die gewünschten HP Zielgeräte bereit.

WICHTIG: Änderungen an den BIOS-Einstellungen erscheinen erst nach einem neuen Inventarscan im Inventar
Allen Änderungen, die Sie bei einem verwalteten HP Gerät durch die Bereitstellung eines Pakets zur Konfiguration der BIOS-Einstellungen vornehmen, spiegeln sich erst *nach* dem nächsten Inventarscan im Inventar des HP Geräts wider.

So erstellen Sie ein Paket mit HP BIOS-Einstellungen

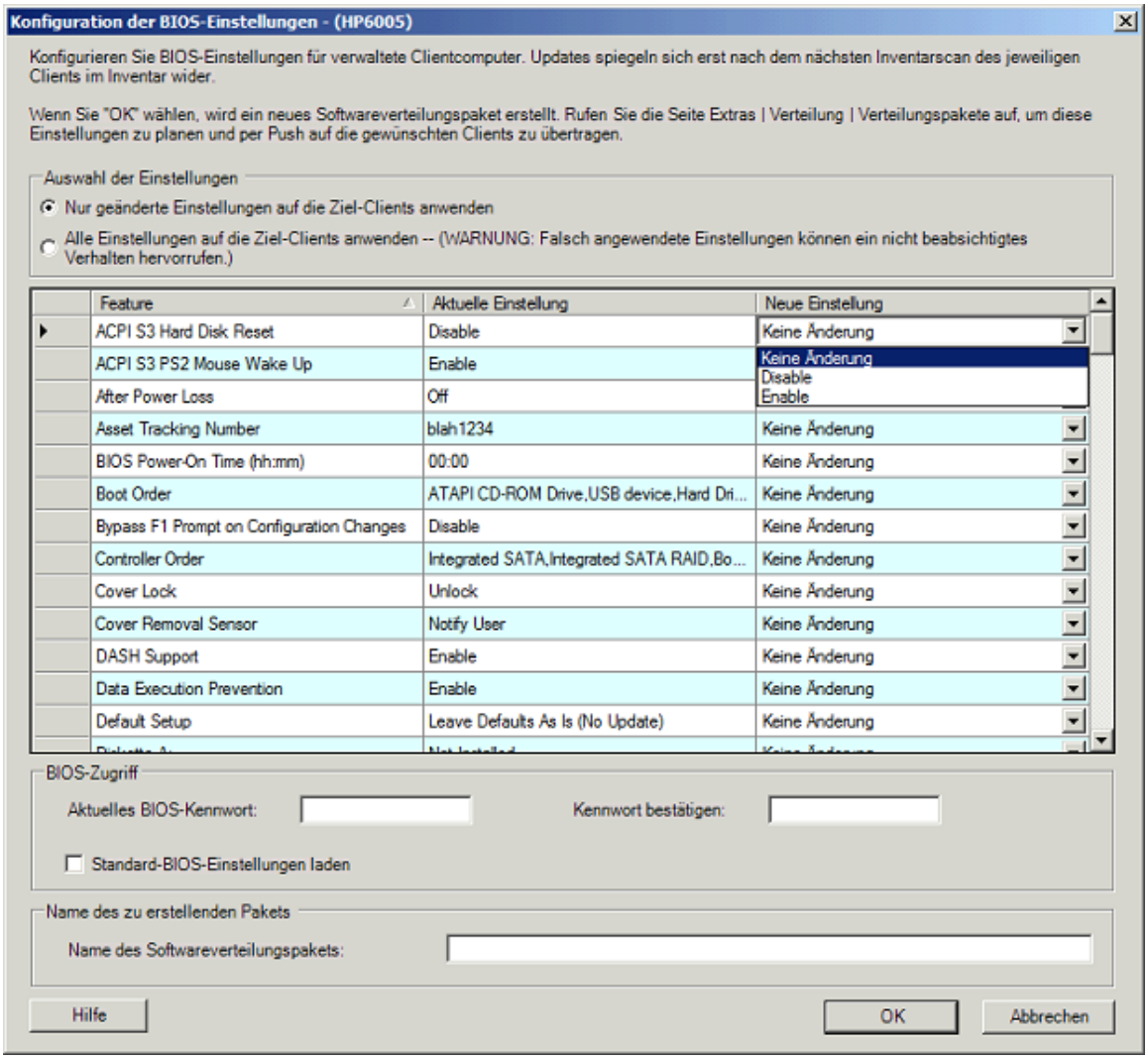
1. Wählen Sie in der Konsole in der Netzwerkansicht das verwaltetes HP Gerät aus.
2. Klicken Sie auf **Extras > Konfigurieren > HP BIOS-Konfiguration**.


Konfiguration der BIOS-Einstellungen - (HPRP5800-2)
Konfigurieren Sie BIOS-Einstellungen für verwaltete Clientcomputer. Updates spiegeln sich erst nach dem nächsten Inventarscan des jeweiligen Clients im Inventar wider.
Wenn Sie "OK" wählen, wird ein neues Softwareverteilungspaket erstellt. Rufen Sie die Seite Extras | Verteilung | Verteilungspakete auf, um diese Einstellungen zu planen und per Push auf die gewünschten Clients zu übertragen.
Auswahl der Einstellungen
Nur geänderte Einstellungen auf die Ziel-Clients anwenden
Alle Einstellungen auf die Ziel-Clients anwenden -- (WARNUNG: Falsch angewendete Einstellungen können ein nicht beabsichtigtes Verhalten hervorrufen.)
Feature
Aktuelle Einstellung
Neue Einstellung
Accessory USB Port 1 Enable Keine Änderung
Accessory USB Port 2 Enable Keine Änderung
Accessory USB Port 3 Enable Keine Änderung
Accessory USB Port 6 Enable Keine Änderung
Accessory USB Port 7 Enable Keine Änderung
Accessory USB Ports Enable Keine Änderung
ACPI S3 PS2 Mouse Wake Up Enable Keine Änderung
After Power Loss Off Keine Änderung
AMT Enable Keine Änderung
Asset Tracking Number 2UA118003P Keine Änderung
BIOS Power-On Time (hh:mm) 00:00 Keine Änderung
BIOS WatchDog Timer <empty> Keine Änderung
Bypass F1 Prompt on Configuration Changes Disable Keine Änderung
BIOS-Zugriff
Aktuelles BIOS-Kennwort:
Kennwort bestätigen:
Standard-BIOS-Einstellungen laden
Name des zu erstellenden Pakets
Name des Softwareverteilungspakets:
Hilfe
OK
Abbrechen

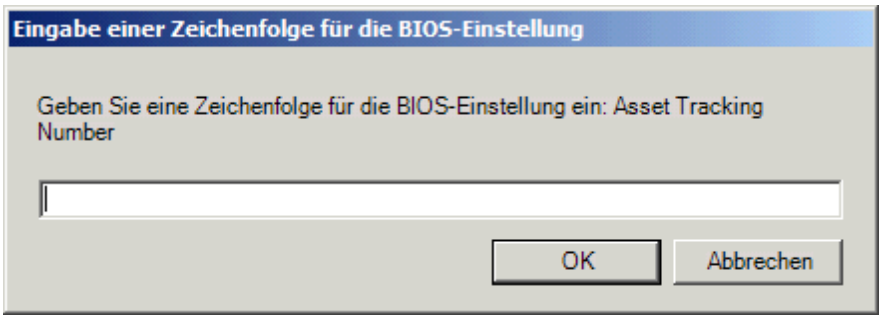
3. Geben Sie einen eindeutigen Namen für das Paket mit den HP BIOS-Einstellungen ein (unten im Dialogfeld.)
4. Wählen Sie, ob *nur* die geänderten BIOS-Einstellungen auf HP Zielgeräte übernommen werden sollen oder ob ALLE BIOS-Einstellungen auf die Zielgeräte angewendet werden sollen.

   WARNUNG: Werden Einstellungen nicht korrekt angewendet, kann dies zu einem nicht beabsichtigten Geräteverhalten führen.

5. Um die Einstellung eines bestimmten BIOS-Features zu ändern, wählen Sie das Feature in der Liste aus und klicken dann in der Spalte "Neue Einstellung" auf die Schaltfläche **Pfeil nach-unten**. Je nach Typ des BIOS-Features wird ein Dropdownmenü angezeigt, an dem Sie die von Ihnen gewünschte Einstellung angeben können, wie im nachstehenden Beispiel gezeigt:



Oder, falls das Feature einen Zeichenfolgenwert erfordert, wird ein Dialogfeld in Form eines Textfelds angezeigt, in das Sie den Wert eingeben könne, wie in diesem Beispiel:


Eingabe einer Zeichenfolge für die BIOS-Einstellung
Geben Sie eine Zeichenfolge für die BIOS-Einstellung ein: Asset Tracking Number
OK
Abbrechen

6. Geben Sie alle BIOS-Einstellungen entsprechend den von Ihnen gewünschten Änderungen oder Aktualisierungen an.
7. Für den Zugriff auf das BIOS des HP-Geräts müssen Sie das aktuelle **BIOS-Kennwort** eingeben und bestätigen.
8. Klicken Sie auf **OK**.

Verwandte Themen

Jetzt können Sie die Konfiguration mithilfe des Extras "Geplante Tasks" bereitstellen Nähere Informationen zur Verwendung des Extras "Geplante Tasks" finden Sie unter:

"Planen von Tasks" auf Seite 242

"Verwenden des Fensters "Geplante Tasks"" auf Seite 243

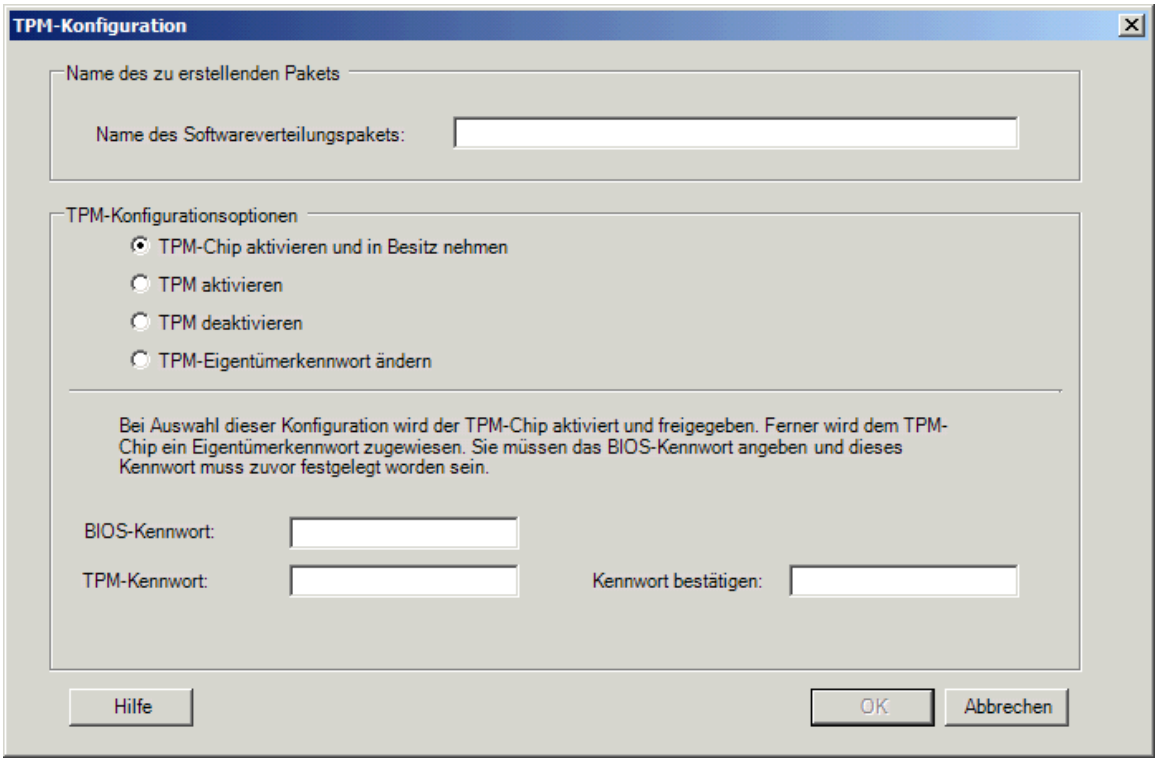
Erstellen und Bereitstellen von HP TPM-Chipeinstellungen für HP Geräte

Dieses Extra können Sie dazu verwenden, die Einstellungen für den Trusted Platform Module (TPM)-Chip auf einem oder mehreren der von Ihnen verwalteten HP Geräte remote zu ändern. Hierzu konfigurieren Sie die TPM-Einstellungen in der LANDesk Konsole und stellen diese Einstellungen dann auf den gewünschten Zielgeräten von HP bereit.

WICHTIG: Windows XP wird nicht unterstützt
Das Extra für die HP TPM-Chipeinstellung wird auf HP Geräten mit dem Betriebssystem Windows XP nicht unterstützt.

So erstellen Sie ein Paket mit HP TPM-Einstellungen

1. Wählen Sie in der Konsole in der Netzwerkansicht ein oder mehrere verwaltete HP Geräte aus.
2. Klicken Sie auf **Extras > Konfigurieren > HP TPM-Konfiguration**.



3. Geben Sie einen eindeutigen Namen für das Paket mit den HP TPM-Konfigurationseinstellungen ein.
4. Wählen Sie eine der folgenden Optionen für den TPM-Chip des HP Geräts: **Aktivieren** oder **Deaktivieren** bzw. **TPM-Chip aktivieren und in Besitz nehmen** oder **Das TPM-Eigentümerkennwort ... ändern**. Je nachdem, welche Option Sie wählen, ändern sich die Steuerelemente unten im Dialogfeld und spiegeln so Ihre Auswahl wider.
5. Um den TPM-Chip in Besitz zu nehmen, müssen Sie das zuvor definiert BIOS-Kennwort eingeben. Für alle anderen Optionen müssen Sie das TPM-Kennwort eingeben.
6. Klicken Sie auf **OK**.

Verwandte Themen

Jetzt können Sie die Konfiguration mithilfe des Extras "Geplante Tasks" bereitstellen Nähere Informationen zur Verwendung des Extras "Geplante Tasks" finden Sie unter:

"Planen von Tasks" auf Seite 242

"Verwenden des Fensters "Geplante Tasks"" auf Seite 243

Verwenden von HP Power Assistant

HP Power Assistant und HP Battery Check helfen Ihnen bei der Steuerung und Optimierung des Energieverbrauchs sowie bei der Leistungssteigerung Ihrer HP Geräte.

Mit HP Power Assistant können Sie die Richtlinien für Stromaktivität und den Energieverbrauch für Ihre verwalteten HP Geräte konfigurieren. Sie können den Energieverbrauch über Ihr Netzwerk hinweg verfolgen, Standardrichtlinien auf alle Ihre HP Geräte anwenden, Kosten sparen und die Produktivität der Endbenutzer steigern.

WICHTIG: Vergewissern Sie sich, dass HP Power Assistent in der richtigen Version vorliegt
Die HP Power Assistant-Software, die Sie installieren, muss die Version 2.1 oder eine höhere Version aufweisen.

Die HP Power Assistant-Optionen werden zur Erstellung einer HP Softwarerichtlinie eingesetzt. Sie verwenden zunächst das Extra HP Softwarerichtlinien zum Konfigurieren von Power Assistant-Einstellungen. Anschließend erfolgt die Zuordnung der Richtlinie zu einem Task vom Typ "Einstellungen ändern" und schließlich die Bereitstellung der (aus HP Power Assistant-Ereignissen bestehenden) Richtlinie für HP Zielgeräte über das Extra "Geplante Tasks".

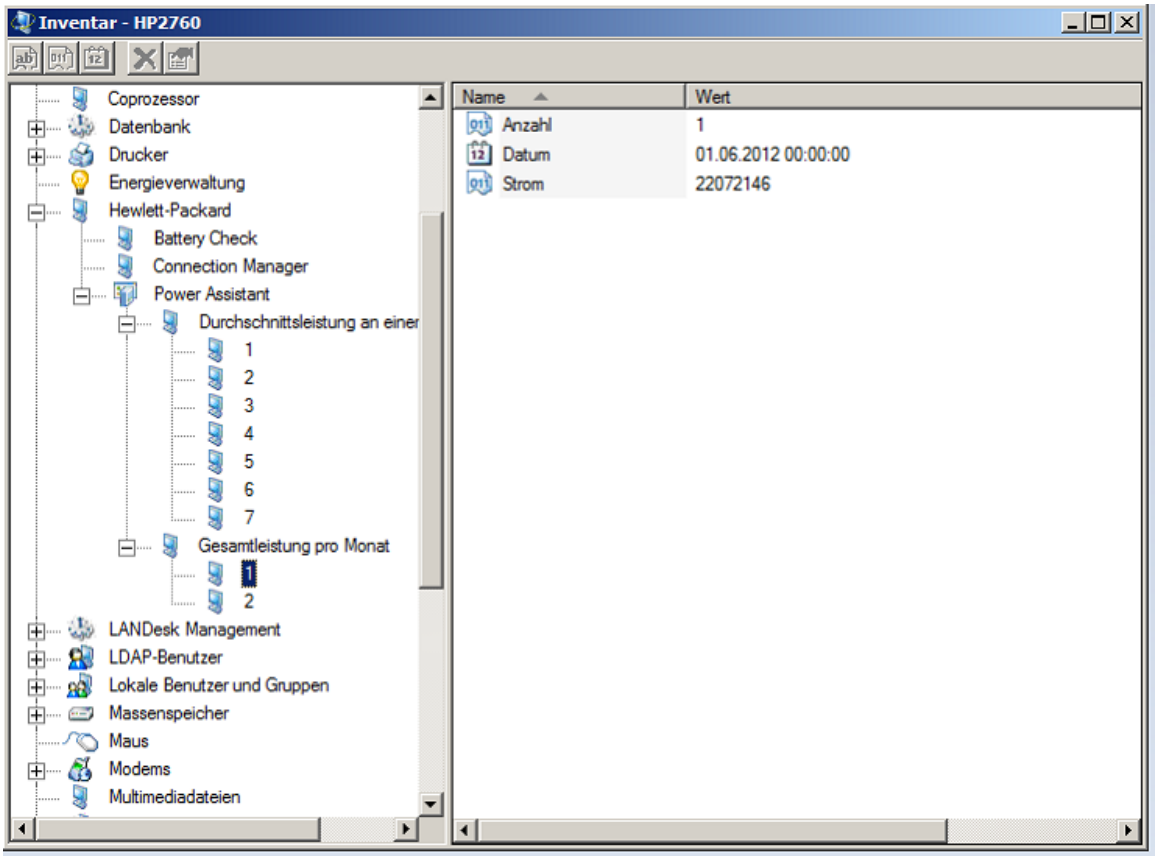
Schrittweise Anleitungen für dieses Verfahren finden Sie unter "Erstellen und Bereitstellen von HP Softwarerichtlinien-Einstellungen für HP Geräte" auf Seite 1015.

Sobald Sie eine HP Power Assistant-Richtlinie für Geräte bereitgestellt haben und diese gescannt wurden, können die Energieverbrauchsdaten im Geräteinventar angezeigt werden. (**HINWEIS:** Diese Daten können auch in den neuen HP spezifischen Berichten im Extra "Berichte" angezeigt werden.)

So zeigen Sie die HP Power Assistant-Daten im Inventar an

1. Wählen Sie in der **Netzwerkansicht** der Konsole ein HP Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Inventar**.

3. Öffnen Sie zunächst den Knoten **Hewlett-Packard** und dann den Knoten **Power Assistant**. Wählen Sie dann eine beliebige Komponente aus, um die Attributwerte einzusehen.



Verwenden von HP Battery Check

HP Battery Check bietet nützliche Informationen zum Batteriezustand und -status Ihres HP Geräts. Mithilfe dieser Informationen können Sie Ihre Investitionen in Hardware optimal ausschöpfen und den Austausch von alten oder defekten Akkus oder Batterien planen und vorbereiten.

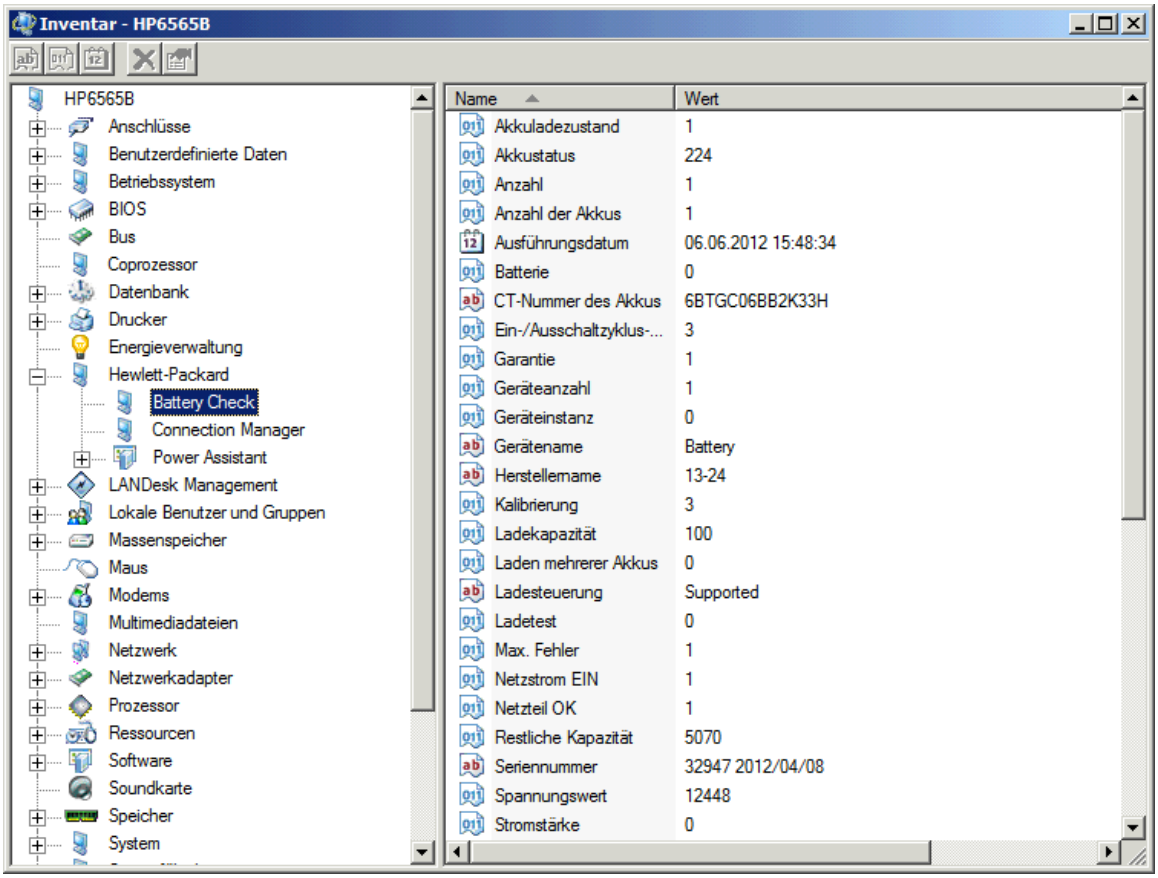
WICHTIG: Vergewissern Sie sich, dass die richtige Version von HP Battery Check installiert ist
Die HP Battery Check-Software, die Sie installieren, muss die Version 4.1 oder eine höhere Version aufweisen.

WICHTIG: HP Battery Check kann nicht auf einem Gerät installiert werden, auf dem bereits HP Support Assistant installiert ist
Um die HP Battery Check-Software installieren zu können, müssen Sie zunächst sicherstellen, dass das Dienstprogramm HP Support Assistant nicht bereits auf dem HP Gerät installiert ist. Fall dies der Fall sein sollte, müssen Sie HP Support Assistant deinstallieren und dann HP Battery Check (Version 4.1 oder höher) installieren.

Im Gegensatz zu HP Power Assistant ist HP Battery Check selbst NICHT konfigurierbar. Der Scanner wird alle 14 Tage ausgeführt und die gescannten Informationen werden in die LANDesk Datenbank eingegeben und können dann im Geräteinventar angezeigt werden. (**HINWEIS:** Diese Daten können auch in den neuen HP spezifischen Berichten im Extra "Berichte" angezeigt werden.)

So zeigen Sie die HP Battery Check-Daten im Inventar an

1. Wählen Sie in der **Netzwerkansicht** der Konsole ein HP Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Inventar**.
3. Öffnen Sie den Knoten **Hewlett-Packard** und wählen Sie **Batterie**, um alle Daten anzuzeigen.



Verwenden von HP Connection Manager

HP Connection Manager bietet nützliche Informationen zu den Netzwerkkarten Ihres HP Geräts. Diese Informationen sind bei der Aktivierung einer Netzwerkkarte sehr hilfreich (Sie können beispielsweise die IMEI-Nummer im Inventar eines gescannten HP Geräts finden, ohne das Gerät dafür öffnen zu müssen), aber auch bei der Verfolgung und Verwaltung der Netzwerkkonnektivität und -aktivität.

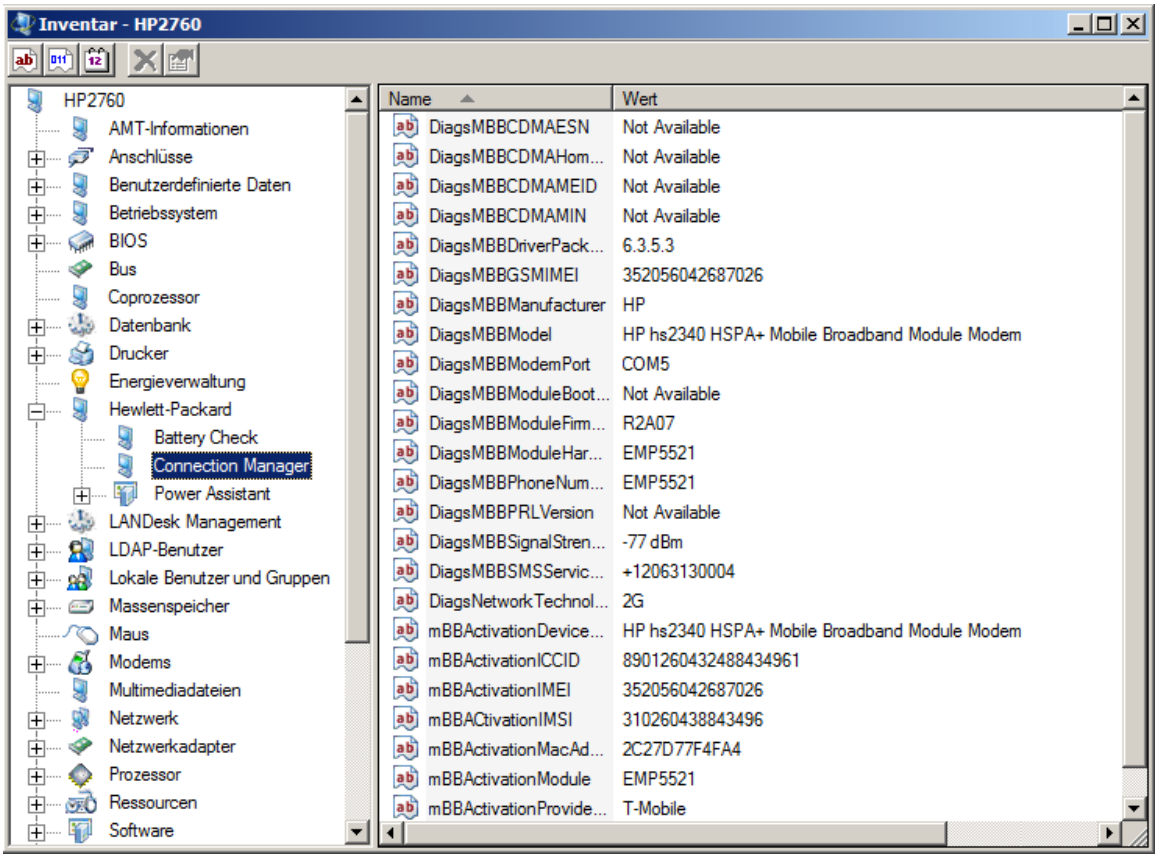
WICHTIG: Vergewissern Sie sich, dass die richtige Version von HP Connection Manager installiert ist
Die von Ihnen installierte Version von HP Connection Manager muss die Version 4.1 oder eine höhere Version sein.

WICHTIG: Unterstützte Netzwerkkarten
HP Connection Manager unterstützt NUR HP kompatible Netzwerkkarten.

Im Gegensatz zu HP Power Assistant ist HP Connection Manager selbst NICHT konfigurierbar. Der Scanner wird einmal pro Tag ausgeführt und die gescannten Informationen werden in die LANDesk Datenbank eingetragen und können dann im Geräteinventar angezeigt werden. (**HINWEIS:** Diese Daten können auch in den neuen HP spezifischen Berichten im Extra "Berichte" angezeigt werden.)

So zeigen Sie die HP Connection Manager-Daten im Inventar an

1. Wählen Sie in der **Netzwerkansicht** der Konsole ein HP Gerät aus.
2. Klicken Sie mit der rechten Maustaste auf das Gerät und klicken Sie dann auf **Inventar**.
3. Öffnen Sie den Knoten **Hewlett-Packard** und wählen Sie **Connection Manager**, um alle Daten anzuzeigen.



Erstellen und Bereitstellen von HP Softwarerichtlinien-Einstellungen für HP Geräte

Die HP Softwarerichtlinien verwenden Sie für die Konfiguration und Bereitstellung der zugehörigen HP Power Assistant-Einstellungen für Ihre verwalteten HP Geräte. Diese Einstellungen ermöglichen Ihnen die Optimierung des Stromverbrauchs und der Leistung mithilfe von standardmäßigen HP Energieverwaltungsaktionen und -profilen, die für bestimmte Zeiten und für eine bestimmte Dauer geplant werden können.

Die HP Standard-Energieverwaltungsaktionen sind:

- Ruhezustand
- Energie sparen
- Ein

Die HP Standard-Energieverwaltungsprofile sind:

- Energiesparmodus
- Ausgewogen
- HP Optimized
- Höchstleistung

Zunächst konfigurieren Sie die Energieeinstellungen mit dem Extra "HP Softwarerichtlinie", weisen dieser gespeicherten Richtlinie einen Task vom Typ "Einstellungen ändern" zu und planen dann die Ausführung des Tasks auf den gewünschten HP Zielgeräten

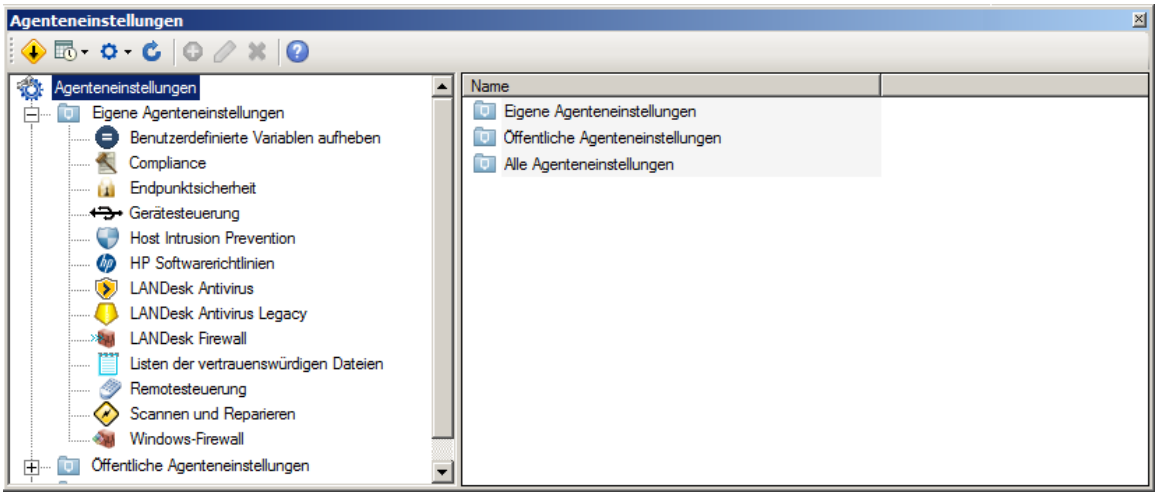
HINWEIS: HP Battery Check und HP Connection Manager werden vom Coreserver ausgeführt
Die Extras "HP Battery Check" und "HP Connection Manager" werden nicht als geplante Tasks von der LANDesk Konsole ausgeführt. Der LANDesk Coreserver führt diese HP Scans automatisch aus und fügt die Daten zur Coredatenbank hinzu. HP Battery Check scannt HP Geräte alle 14 Tage. HP Connection Manager scannt HP Geräte einmal pro Tag.

HP Softwarerichtlinien sind Teil des Extras "Sicherheitskonfigurationen" (**Extras > Sicherheit und Compliance > Sicherheitskonfigurationen**).

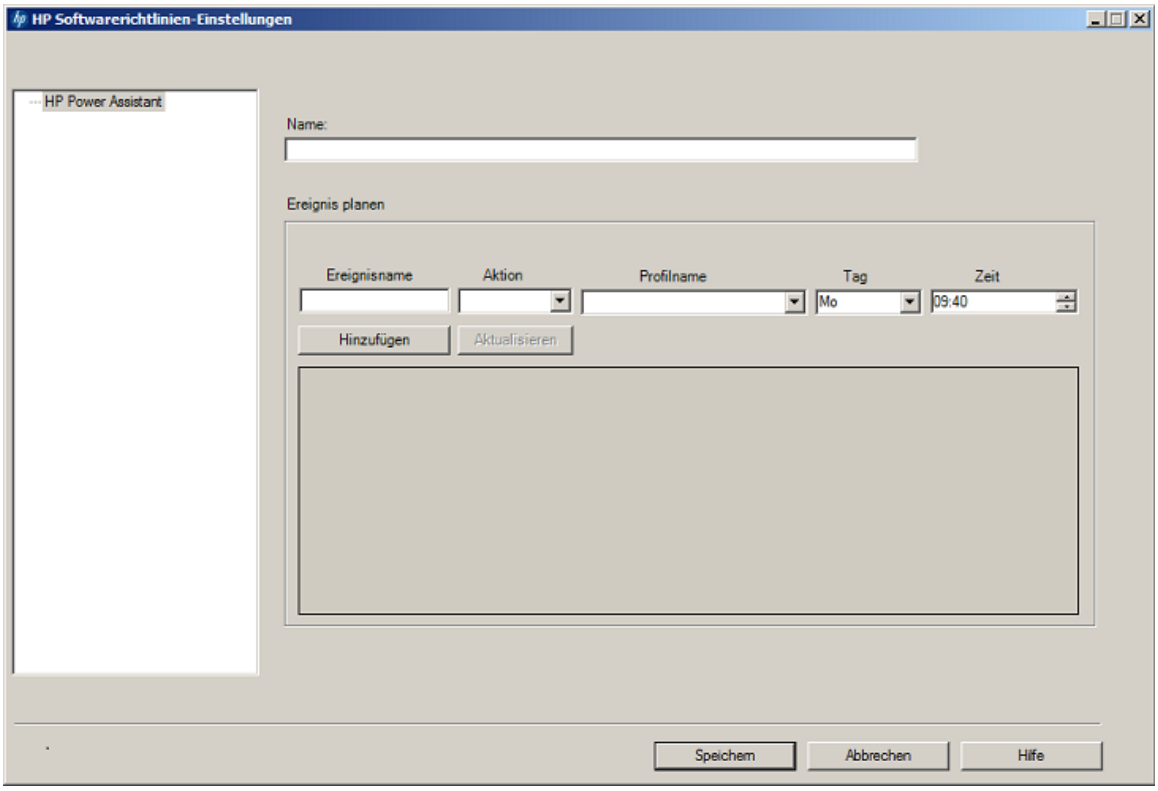
WICHTIG: Änderungen an den HP Power Assistant-Einstellungen erscheinen erst nach einem neuen Inventarscan im Inventar
Allen Änderungen, die Sie bei einem verwalteten HP Gerät durch die Bereitstellung eines HP Softwarerichtlinien-Tasks (von Typ "Einstellungen ändern") vornehmen, spiegeln sich erst *nach* dem nächsten Inventarscan im Inventar des HP Geräts wider.

So erstellen Sie ein Paket mit HP Softwarerichtlinien-Einstellungen (für Power Assistant)

1. Öffnen Sie in der Konsole das Extra **Sicherheitskonfigurationen**.
2. Doppelklicken Sie auf **Eigene Sicherheitskonfigurationen**.



3. Klicken Sie mit der rechten Maustaste auf **HP Softwarerichtlinien** und dann auf **Neu**. Das Dialogfeld HP Softwarerichtlinien-Einstellungen wird angezeigt. Hier konfigurieren Sie die HP Power Assistant-Einstellungen, die den Energiemodus bei den verwalteten HP Geräten steuern.

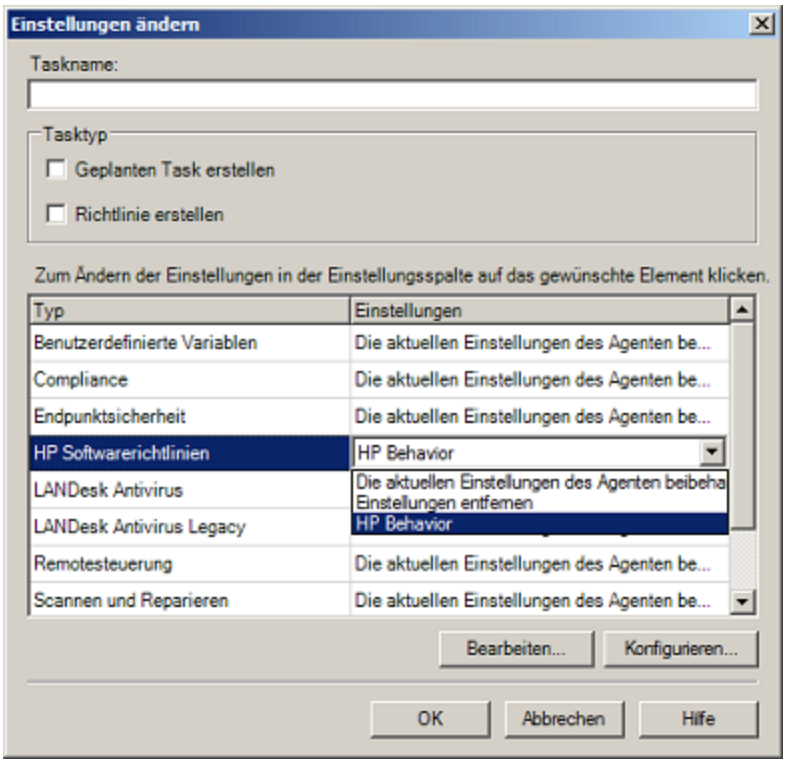


4. Geben Sie einen eindeutigen Namen für das Paket mit den HP Softwarerichtlinien-Einstellungen ein.
5. Geben Sie einen eindeutigen Namen für das spezifische Ereignis ein, das Sie konfigurieren. Ein Einstellungspaket kann ein oder mehrere Ereignisse umfassen, die für unterschiedliche Tage und/oder Zeiträume geplant sind.
6. Wählen Sie im Menü **Aktion** den Typ der Aktion aus, die von diesem Ereignis durchgeführt werden soll (Ruhezustand, Energie sparen, Ein).
7. Wählen Sie im Menü **Profilname** das vordefinierte HP Energieprofil aus, das von diesem Ereignis implementiert werden soll (Energiesparmodus, Ausgewogen, Optimized, Höchstleistung).
8. Geben Sie über die Menüs für **Datum** und **Zeit** an, wann dieses Ereignis angewendet werden soll.
9. Klicken Sie auf **Hinzufügen**, um dieses Ereignis zum Listenfeld hinzuzufügen. Eine HP Softwarerichtlinie und die zugehörigen HP Power Assistant-Einstellungen werden durch diese Kombination eines oder mehrerer Ereignisse definiert.
10. Wenn Sie die Konfiguration der HP Softwarerichtlinie bzw. HP Power Assistant-Richtlinie abgeschlossen haben, klicken Sie auf **Speichern**, um die Einstellungen zu speichern und das Dialogfeld zu schließen. Die neue Richtlinie erscheint daraufhin im rechten Fensterausschnitt.

Jetzt können Sie die Richtlinie bereitstellen, indem Sie sie einem Task von Typ "Einstellungen ändern" zuweisen und dann mit dem Extra "Geplante Tasks" den Zeitpunkt und die HP Zielgeräte festlegen.

So erstellen Sie einen Task vom Typ "Einstellungen ändern" mit einer HP Softwarerichtlinie

1. Klicken Sie im Fenster "Sicherheitskonfigurationen" auf die Symbolleistenschaltfläche **Task erstellen** und klicken Sie dann auf **Einstellungen ändern**.



2. Geben Sie einen eindeutigen Namen für den Task ein.
3. Geben Sie an, ob Sie einen geplanten Task oder eine Richtlinie erstellen wollen.
4. Wählen Sie im Dropdownmenü für **HP Softwarerichtlinien**-Einstellungen die Richtlinie aus, die für die Zielgeräte bereitgestellt werden sollen.
5. Klicken Sie auf **OK**, um den Task zu speichern und das Dialogfeld zu schließen.

Verwandte Themen

Jetzt können Sie die Konfiguration mithilfe des Extras "Geplante Tasks" bereitstellen. Nähere Informationen zur Verwendung des Extras "Geplante Tasks" finden Sie unter:

"Planen von Tasks" auf Seite 242

"Verwenden des Fensters "Geplante Tasks"" auf Seite 243

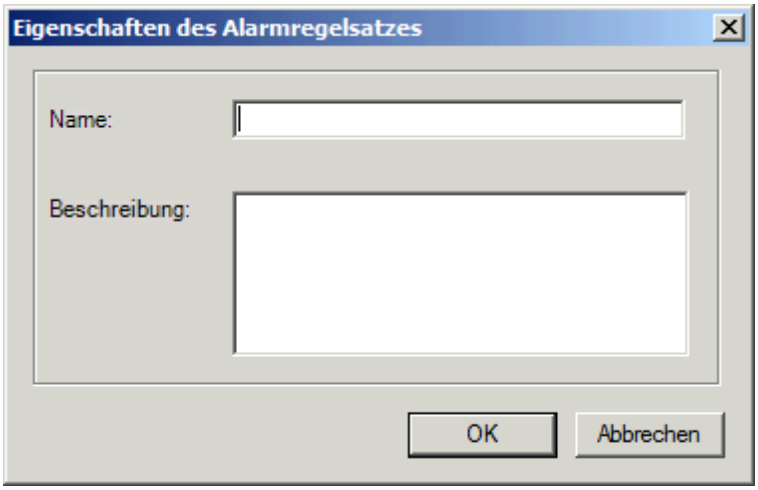
Konfigurieren von Alarmen für verwaltete HP Geräte

Sie können das LANDesk Extras "Alarmierung" zur Erstellung von *Alarmregelsätzen* verwenden, die der Überwachung und Messung dienen und Sie alarmieren, wenn auf Ihren verwalteten HP Geräten und RPOS-Geräten ein definiertes Ereignis eintritt, eine Bedingung erfüllt ist oder ein Grenzwert überschritten wurde.

Benutzerdefinierte Regelsätze lösen Alarme aus, um Sie zu benachrichtigen, wenn bei Attributen von Komponenten eines HP Geräts oder Retail Point-of-Sale (RPOS)-Geräts ein von Ihnen festgelegter Grenzwert – wie die Spannung, Temperatur, Anzahl der gedruckten Seiten usw. –überschritten wurde.

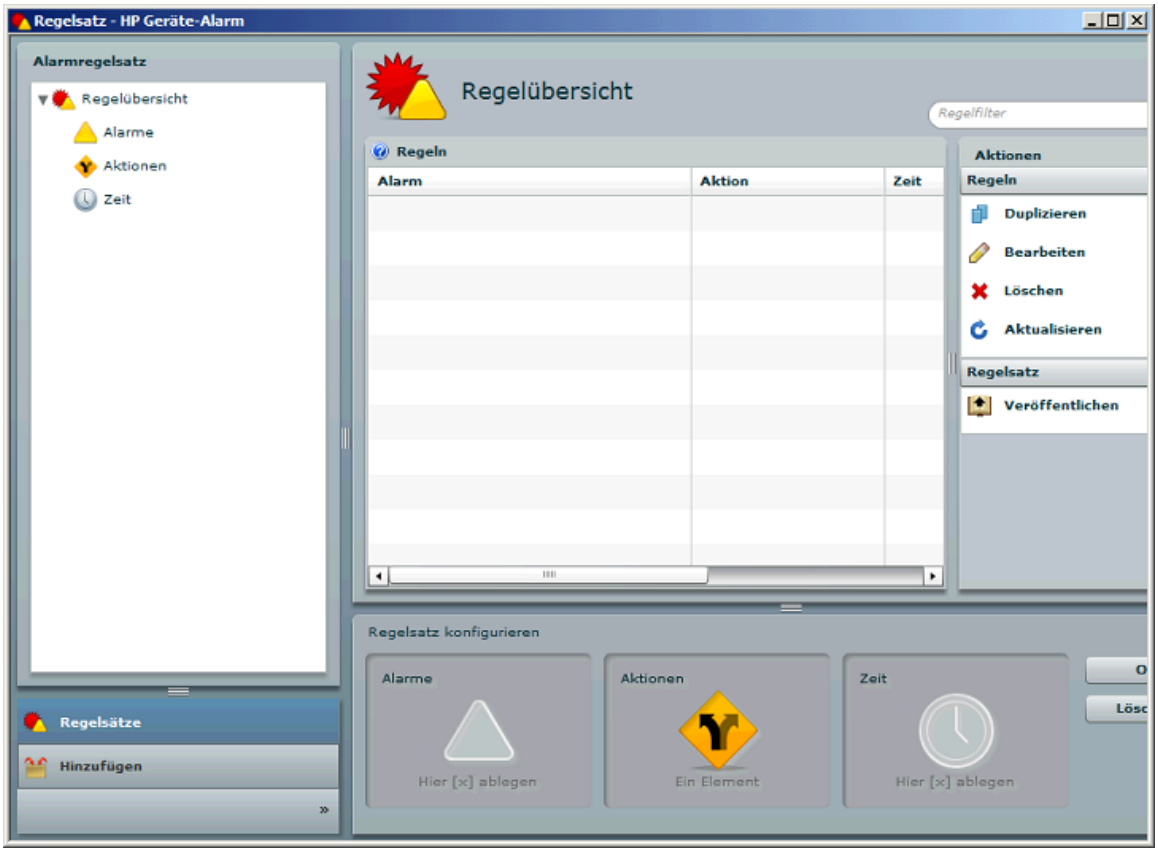
So konfigurieren Sie Alarme und Alarmregelsätze

1. Klicken Sie in der Konsole auf **Extras > Konfiguration > Alarmierung** Das Fenster des Extras "Alarmierung" wird angezeigt.
2. Klicken Sie in der Symbolleiste auf **Neuer Alarmregelsatz**.



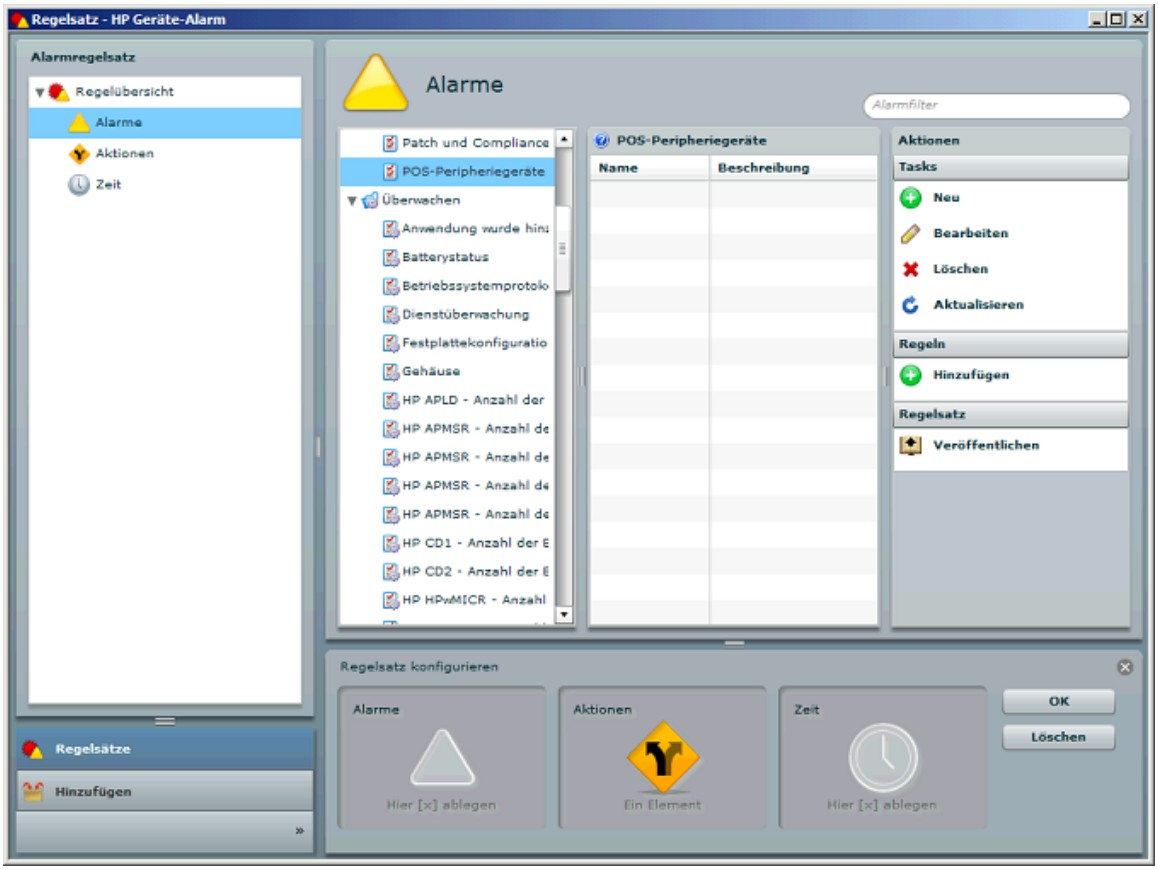
3. Geben Sie einen eindeutigen Namen und eine Beschreibung für den neuen Regelsatz ein, und klicken Sie auf **OK**. Der neue Regelsatz wird in der Liste der Alarme angezeigt.

4. Klicken Sie mit der rechten Maustaste auf den Regelsatz und klicken Sie dann auf **Bearbeiten**.

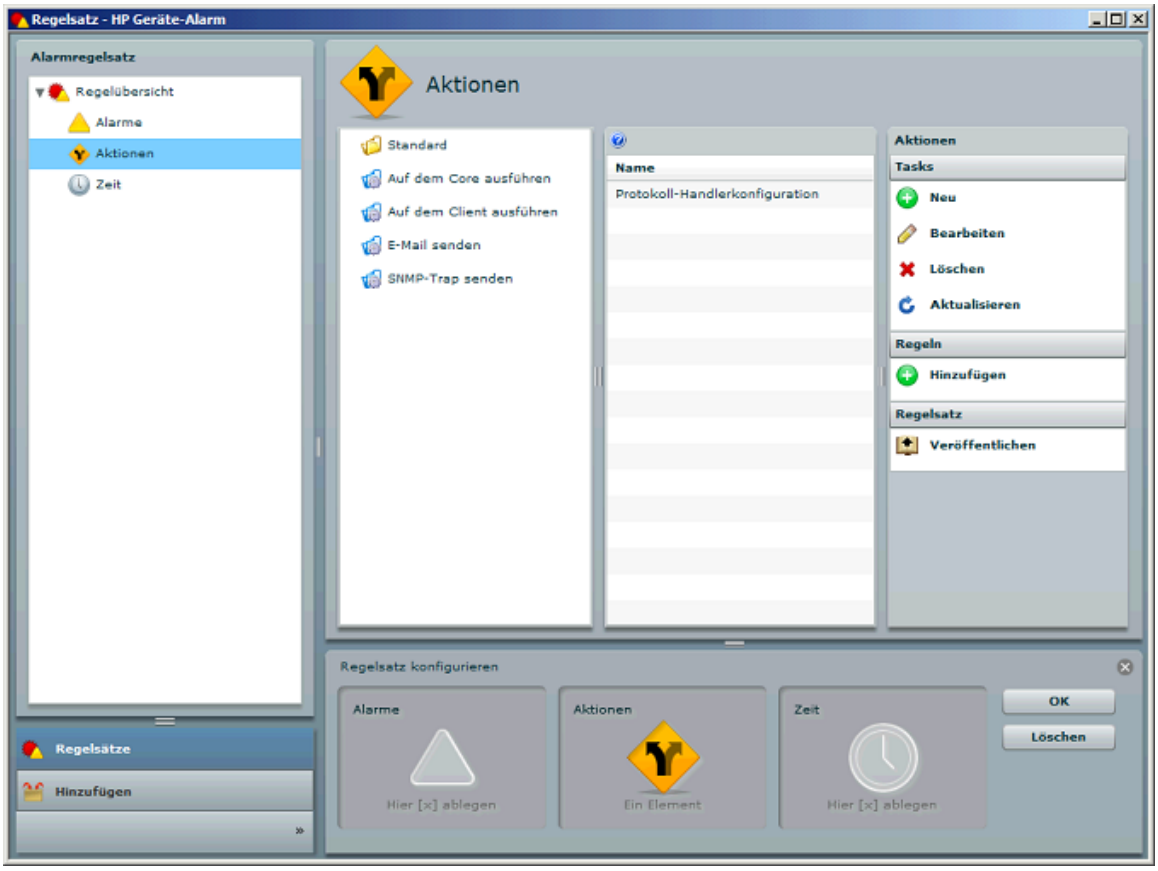


5. Klicken Sie im Dialogfeld "Regelübersicht" auf **Alarme**, um die Liste der Alarme zu öffnen. Dort können Sie das Element auswählen, für das eine Alarmierung erfolgen soll.

   Der Alarm für POS-Peripheriegeräte befindet sich unter dem Knoten **Standard**. Mehrere HP Geräte und RPOS-Peripheriegeräte sowie Attribute befinden Sie unter dem Knoten **Bildschirm**. Suchen Sie in dieser Liste nach der Komponente oder dem Feature, das Sie verfolgen und bezüglich dessen Sie alarmiert werden möchten.



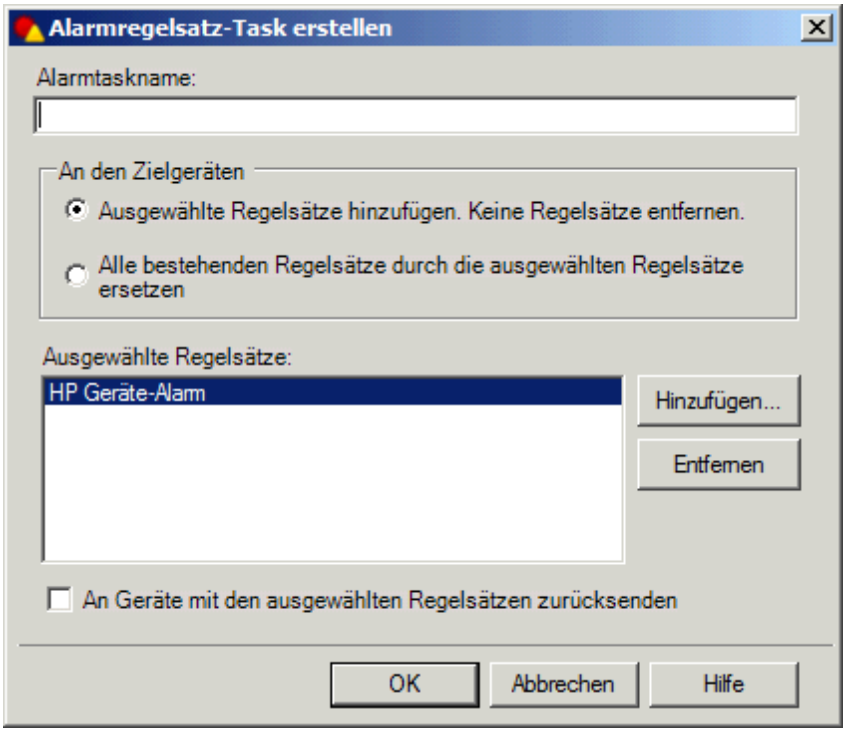
6. Klicken Sie auf **Aktionen**, um den Bereich "Aktionen" zu öffnen, in dem Sie das Alarmierungsverhalten festlegen können.



7. Klicken Sie auf **Zeit**, um den Bereich mit den Zeitoptionen aufzurufen, in dem Sie die Zeiteinstellungen für diesen Alarm angeben können.

8. Klicken Sie auf **Hinzufügen**, um den soeben konfigurierten Alarm zum Regelsatz hinzuzufügen.
9. Wenn Sie die Erstellung Ihres Regelsatzes abgeschlossen haben, klicken Sie auf **OK**.

10. Klicken Sie im Fenster des Extras "Alarmierung" mit der rechten Maustaste auf den Alarmregelsatz, den Sie für die HP Zielgeräte bereitstellen möchten, und klicken Sie dann auf **Regelsätze verteilen**. (Sie können aber auch in der Symbolleiste auf **Task erstellen** und anschließend auf **Regelsätze verteilen** klicken.



11. Geben Sie einen Namen für den Alarm-Task ein und entscheiden Sie, ob die ausgewählten Regelsätze zu den auf dem Zielgerät eventuell bereits vorhandenen Regelsätzen hinzugefügt werden sollen. Klicken Sie dann auf **Hinzufügen** oder **Entfernen**, um die Regelsätze anzupassen, die mit diesem Task verteilt werden sollen, und klicken Sie dann auf **OK**, um den Task zu erstellen und ihn zum Fenster des Extras Geplante Tasks hinzuzufügen.

Jetzt können Sie das Extra "Geplante Tasks" verwenden, um den Task für den Alarmregelsatz für die gewünschten HP Zielgeräte bereitzustellen. Detaillierte Informationen zur Verwendung des Extras "Geplante Tasks" finden Sie unter "Planen von Tasks" auf Seite 242 und "Verwenden des Fensters "Geplante Tasks"" auf Seite 243.

HINWEIS: Verwenden des LANDesk Extras Alarmierung
Ausführliche Informationen zur Verwendung des LANDesk Extras "Alarmierung" finden Sie im *Benutzerhandbuch* in dem Abschnitt "Alarmfunktion" auf Seite 832.

Generieren von Berichten für verwaltete HP Geräte

Mit dem Extra LANDesk Berichte können Sie Berichte mit kritischen und aktuellen Informationen generieren, die Sie zum Identifizieren und Lösen von Problemen, zur Verfolgung Ihrer HP Geräte und damit verbundenen Retail POS-Peripheriegeräte sowie zur Aufzeichnung und gemeinsamen Nutzung dieser wichtigen Informationen mit anderen wichtigen Beteiligten verwenden können.

Mit dem Extra "Berichte" können Sie Echtzeitberichte ausführen, geplante Berichtstasks erstellen und Berichte (als PDF-, XLS-, DOC- oder CSV-Datei) exportieren.

Berichtsarten, die mit dem Extra "Berichte" erstellt werden können:

- Standardberichte (Inventar)
- HP spezifische Berichte (Anbieter)
- Benutzerdefinierte Berichte auf der Basis von Datenbankabfragen

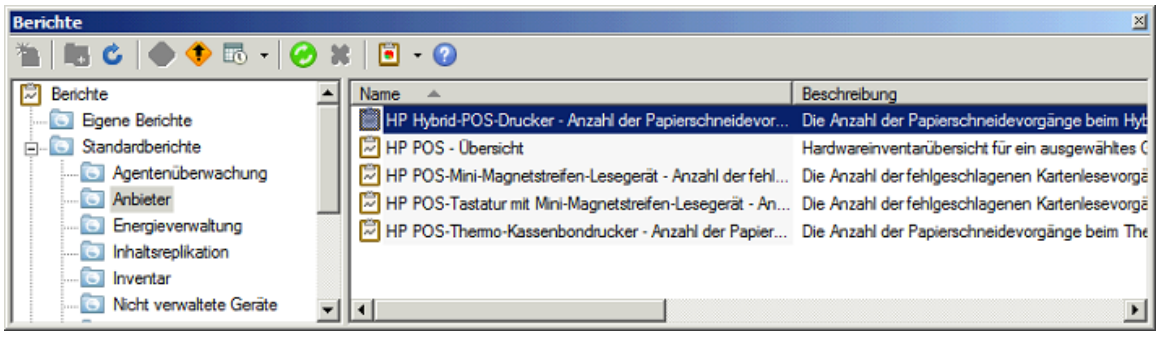
HP Berichte

Das integrierte Extra "LANDesk plus HP Hardware and Software Management" umfasst mehrere vordefinierte HP spezifische Berichte, die zum Extra "Berichte" hinzugefügt werden, wenn Sie die HP Software installieren.

Die HP Berichte sind:

- [NEU] HP Akkuzustandsüberprüfung (mit Daten, die aus einem HP Diagnosescan zur Überprüfung des Akkus stammen, siehe "Verwenden von HP Battery Check" auf Seite 1013)
- [NEU] HP Mobile Broadband-Karte - Assetinformationen (mit Daten, die aus einem HP Connection Manager-Scan stammen, siehe "Verwenden von HP Connection Manager" auf Seite 1014)
- HP Hybrid-POS-Drucker - Anzahl der Papierschneidevorgänge
- HP POS-Tastatur mit Mini-Magnetstreifen-Lesegerät - Anzahl der fehlgeschlagenen Kartenlesevorgänge
- HP POS-Mini-Magnetstreifen-Lesegerät - Anzahl der fehlgeschlagenen Kartenlesevorgänge
- HP POS - Übersicht
- HP POS-Thermo-Kassenbondrucker - Anzahl der Papierschneidevorgänge
- [NEU] HP Power Assistant – Energieverbrauch (mit Daten, die aus einem benutzerdefinierten Task für HP Softwarerichtlinien-Einstellungen stammen, siehe "Erstellen und Bereitstellen von HP Softwarerichtlinien-Einstellungen für HP Geräte" auf Seite 1015)
- [NEU] HP Power Assistant – Energieverbrauch nach Wochentag (mit Daten, die aus einem benutzerdefinierten Task für HP Softwarerichtlinien-Einstellungen stammen, siehe "Erstellen und Bereitstellen von HP Softwarerichtlinien-Einstellungen für HP Geräte" auf Seite 1015)

Diese HP Berichte finden Sie im Fenster des Extras "Berichte" unter **Standardberichte >** Gruppe **Anbieter**.



Generieren von Berichten

So generieren Sie Berichte

1. Klicken Sie in der Konsole auf **Extras > Berichte / Überwachung > Berichte**. Das Fenster des Extras "Berichte" wird angezeigt.
2. Zum Ausführen (und Verwalten) von Standardinventarberichten öffnen Sie in der Strukturansicht **Berichte**, die Gruppe **Standardberichte**. Klicken Sie auf die Gruppe **Inventar** und mit der rechten Maustaste auf einen bestimmten Bericht in der Liste im rechten Fensterausschnitt und klicken Sie dann auf **Ausführen**. Geben Sie die Berichtsparameter an und klicken Sie dann auf **Bericht anzeigen**.
3. Zum Ausführen (und Verwalten) von HP spezifischen Berichten öffnen Sie in der Strukturansicht **Berichte**, die Gruppe **Standardberichte**. Klicken Sie auf die Gruppe **Anbieter** und mit der rechten Maustaste auf einen spezifischen HP Bericht in der Liste der Berichte (siehe obige Abbildung) und klicken Sie dann auf **Ausführen**. Geben Sie die Berichtsparameter an und klicken Sie dann auf **Bericht anzeigen**.
4. Zum Erstellen (und Verwalten) eines benutzerdefinierten, abfragebasierten Berichts klicken Sie mit der rechten Maustaste auf **Eigene Berichte** und klicken Sie dann auf **Neuer Bericht**. Geben Sie einen eindeutigen Titel und eine Beschreibung ein. Klicken Sie auf **Aus LDMS-Abfrage abrufen**, wählen Sie die Datenbankabfrage aus, die Sie als Kriterium für Ihren benutzerdefinierten Bericht verwenden möchten und klicken Sie dann auf **OK**. Geben Sie andere Berichtsoptionen wie gewünscht an und klicken Sie dann auf **OK**, um den Bericht zu erstellen und ihn in der Gruppe "Eigene Berichte" zu speichern.

Zur Erstellung von benutzerdefinierten Berichten müssen Sie zunächst Datenbankabfragen erstellen, die auf HP gerätespezifischen Daten (und/oder HP Retail-POS-Gerätedaten) aufbauen. Diese Abfragen erstellen Sie mit dem Extra "Abfragen" in der Netzwerkansicht der Konsole.

HINWEIS: Verwenden des LANDesk Extras "Abfragen"
Ausführliche Informationen zur Verwendung des LANDesk Extras "Abfragen" finden Sie im *Benutzerhandbuch* in dem Abschnitt zu Abfragen, der mit "Abfragen/Verzeichnis-Manager" auf Seite 193 überschrieben ist.

HINWEIS: Verwenden des LANDesk Extras "Berichte"
Ausführliche Informationen zur Verwendung des LANDesk Extras "Berichte" finden Sie im *Benutzerhandbuch* in dem Abschnitt zu Berichten der mit "Berichte" auf Seite 209überschrieben ist.

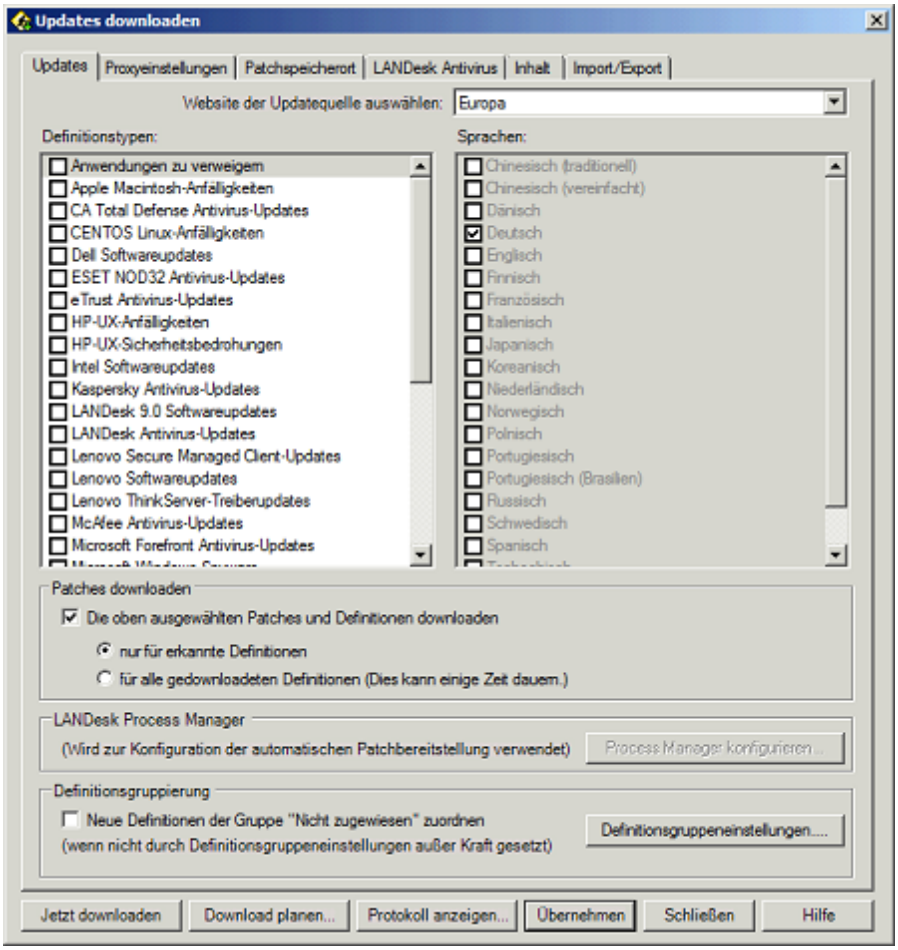
Herunterladen und Bereitstellen von HP Software- bzw. Treiberupdates

Sie können das LANDesk Management Suite-Extra "Patch und Compliance" für den Download der neuesten HP Treiberpacks und HP BIOS-Inhaltsupdates (d. h. "HP Softpaq"-Updates) verwenden und diese für Ihre verwalteten HP Geräte bereitstellen.

WICHTIG: Ein separates HP spezifisches Inhaltsabonnement ist NICHT erforderlich
Sie benötigen KEIN separates spezielles Inhaltsabonnement für den Download des HP spezifischen Inhalts mit dem LANDesk Extra "Patch und Compliance - Updates downloaden". HP Hardware and Software Management-Inhalte (HP Softpaq-Updates) gelten als LANDesk Standardinhalt und stehen daher im Rahmen des LANDesk Software-Basisabonnements zum Download zur Verfügung.

So laden Sie HP Updates herunter

1. Klicken Sie in der Konsole auf **Extras > Sicherheit und Compliance > Patch und Compliance**. Das Fenster des Extras "Patch und Compliance" wird angezeigt.
2. Klicken Sie in der Symbolleiste auf die Schaltfläche **Updates downloaden**.



3. Wählen Sie in der Liste der Definitionstypen den Eintrag **HP Updates** aus.
4. Klicken Sie auf **Jetzt herunterladen**, um den Downloadvorgang sofort zu starten.

   ODER

   Klicken Sie auf **Download planen**, um einen geplanten Download-Task im Extra "Geplante Tasks" zu erstellen.
5. Sobald der Download der HP Softwareupdates abgeschlossen ist, können Sie das Extra "Patch und Compliance" verwenden, um den Inhalt anzuzeigen, zu filtern und zu einem Sicherheits-/Compliancescantask hinzufügen, um die HP Softwareupdates für Ihre verwalteten HP Geräte bereitzustellen.

HINWEIS: Verwenden des LANDesk Extras "Patch und Compliance"
Ausführliche Informationen zur Verwendung des LANDesk Extras "Patch und Compliance" finden Sie im

Benutzerhandbuch in dem Abschnitt zum Download von Updates, der mit "Download von Updates für Sicherheitsinhalte" auf Seite 600 beginnt.

Verwalten von HP Thin Client-Geräten über die LANDesk Konsole

Sobald Ihre HP Thin Client-Geräte mit dem Standard LANDesk Agenten konfiguriert und in die LANDesk Datenbank und das LANDesk Inventar eingescannt wurden, können Sie einige der gängigsten LANDesk Extras zur Verfolgung und Verwaltung dieser Geräte verwenden.

Die nachstehende Liste gibt Aufschluss über die unterstützten HP Thin Client-Plattformen sowie die LANDesk Features, Funktionen und Extras, die für die jeweilige Plattform bereitgestellt werden. Außerdem finden Sie dort eine kurze Beschreibung zu jedem Extra und einen Link zum jeweiligem Hauptübersichtsthema in der Hilfe.

Unterstützte HP Thin Client-Betriebssystemplattformen

LANDesk Management Suite Version 9.5 bietet für die folgenden unterstützten HP Thin Client-Plattformen die jeweils aufgeführten spezifischen Funktionen.

Windows Embedded Standard 7 Enterprise (WES 7)

- Standard LANDesk Agentenkonfiguration (Inventar, Abfragen)
- Remotesteuerung
- Softwareverteilung
- Patchmanagement
- Schreibfilterverwaltung

Windows Embedded Standard 09 Enterprise (WES 09)

- Standard LANDesk Agentenkonfiguration (Inventar, Abfragen)
- Remotesteuerung
- Softwareverteilung
- Patchmanagement
- Schreibfilterverwaltung

HP ThinPro (Ubuntu)

- Standard LANDesk Agentenkonfiguration (Inventar, Abfragen)

Hilfe zur Konfiguration der BIOS-Einstellungen

Dies ist ein kontextbezogenes Hilfethema zum Dialogfeld "Konfiguration der BIOS-Einstellungen" in der LANDesk Konsole.

Dieses Dialogfeld verwenden Sie zum Konfigurieren von BIOS-Einstellungen, die Sie dann für Ihre verwalteten HP Geräte bereitstellen können.

WICHTIG: Änderungen an den Einstellungen erscheinen erst nach einem neuen Inventarscan im Inventar
Alle Änderungen, die Sie in diesem Dialogfeld vornehmen und für ein HP Zielgerät bereitstellen, spiegeln

sich erst *nach* dem nächsten Inventarscan im Inventar des Geräts wider.

Dieses Dialogfeld enthält folgende Optionen:

- **Auswahl der Einstellungen:**
  - **Nur geänderte Einstellungen auf die Ziel-Clients anwenden:** Stellt sicher, dass nur die BIOS-Einstellungen, die Sie mit dieser Konfiguration geändert haben, auf die HP Zielgeräte übernommen werden.
  - **Alle Einstellungen auf die Ziel-Clients anwenden:** Stellt sicher, dass *alle* in dieser Konfiguration enthaltenen BIOS-Einstellungen auf die HP Zielgeräte übernommen werden.
- **Featureliste:**
  - **Feature:** Der Name der HP BIOS-Komponente
  - **Aktuelle Einstellung:** Der Wert der angegebenen HP BIOS-Komponente auf der Basis des letzten Inventarscans.
  - **Neue Einstellung:** Der geänderte Wert, der für die angegebene HP BIOS-Komponente übernommen werden soll.
- **BIOS-Zugriff:**
  - **Aktuelles BIOS-Kennwort:** Gewährt Zugriff auf die HP BIOS-Daten.
  - **Kennwort bestätigen:** Erforderlich für den Zugriff auf die HP BIOS-Daten.
  - **Standard-BIOS-Einstellungen laden:** Löscht die vorhandenen Werte der HP BIOS-Komponenten und setzt diese auf die Systemstandardwerte zurück.
- **Name des zu erstellenden Pakets:**
  - **Name des Softwareverteilungspakets:** Kennzeichnet des Softwarepaket mit einem eindeutigen Namen.
- **OK:** Schließt das Dialogfeld und speichert das Softwarepaket im Extra "LANDesk Softwareverteilung".
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwandte Themen

Schrittweise Anleitungen für die Konfiguration von HP BIOS-Einstellungen, die für Zielgeräte bereitgestellt werden können, finden Sie unter "Erstellen und Bereitstellen von HP BIOS-Einstellungen für HP Zielgeräte" auf Seite 1007.

Hilfe zur TPM-Konfiguration

Dies ist ein kontextbezogenes Hilfethema zum Dialogfeld "TPM-Konfiguration" in der LANDesk Konsole.

Dieses Dialogfeld verwenden Sie zum Konfigurieren von Einstellungen für den TPM (Trusted Platform Module)-Sicherheitschip, die Sie dann für Ihre verwalteten HP Geräte bereitstellen können.

WICHTIG: Windows XP wird nicht unterstützt
Das Extra für die HP TPM-Chipeinstellung wird auf HP Geräten mit dem Betriebssystem Windows XP nicht unterstützt.

WICHTIG: Änderungen an den Einstellungen erscheinen erst nach einem neuen Inventarscan im Inventar
Alle Änderungen, die Sie in diesem Dialogfeld vornehmen und für ein HP Zielgerät bereitstellen, spiegeln sich erst nach dem nächsten Inventarscan im Inventar des Geräts wider.

Dieses Dialogfeld enthält folgende Optionen:

- **Name des Softwareverteilungspakets:** Kennzeichnet des Softwarepaket mit einem eindeutigen Namen.
- **TPM-Konfigurationsoptionen** Legt die Einstellungen des HP TPM-Sicherheitschips auf dem HP Zielgerät fest. (**HINWEIS:** Je nachdem, welche Option Sie auswählen, ändern sich die nachstehenden Kennwortfelder für den Zugriff auf TPM-Daten und die Übernahme der neuen Einstellung.)
- **BIOS-Kennwort:** Gewährt Zugriff auf die HP BIOS-Daten.
- **TPM-Kennwort:** Gewährt Zugriff auf die HP TPM-Daten.
- **Kennwort bestätigen:** Erforderlich für den Zugriff auf die entsprechenden Daten.
- **OK:** Schließt das Dialogfeld und speichert das Softwarepaket im Extra "LANDesk Softwareverteilung".
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwandte Themen

Schrittweise Anleitungen für die Konfiguration von HP BIOS-Einstellungen, die für Zielgeräte bereitgestellt werden können, finden Sie unter "Erstellen und Bereitstellen von HP TPM-Chipeinstellungen für HP Geräte" auf Seite 1010.

Hilfe zu den HP Softwarerichtlinien-Einstellungen

Dies ist ein kontextbezogenes Hilfethema zum Extra "HP Softwarerichtlinien-Einstellungen" in der LANDesk Konsole.

Dieses Dialogfeld verwenden Sie zum Konfigurieren von HP Power Assistant-Einstellungen, die Sie dann für Ihre verwalteten HP Geräte bereitstellen können.

WICHTIG: Änderungen an den Einstellungen erscheinen erst nach einem neuen Inventarscan im Inventar
Alle Änderungen, die Sie in diesem Dialogfeld vornehmen und für ein HP Zielgerät bereitstellen, spiegeln sich erst nach dem nächsten Inventarscan im Inventar des Geräts wider.

Dieses Dialogfeld enthält folgende Optionen:

- **Name:** Kennzeichnet die Richtlinieneinstellungen mit einem eindeutigen Namen.
- **Ereignis planen:**
  - **Ereignisname:** Kennzeichnet ein bestimmtes Ereignis in der HP Power Assistant-Richtlinie. Sie können ein oder mehrere Ereignisse hinzufügen, um eine benutzerdefinierte Energierichtlinie zu erstellen.
  - **Aktion:** Gibt die Aktion an, die von diesem Ereignis ausgeführt wird (Ruhezustand, Energie sparen, Ein).
  - **Profilname:** Gibt das HP Standard-Energieprofil (Energiesparmodus, Ausgewogen, HP Optimized, Höchstleistung) für das Ereignis an, das Sie gerade definieren.
  - **Tag:** Gibt an welchem Tag bzw. an welchen Tagen dieses Ereignis auf den Zielgeräten aktiviert wird.
  - **Zeit:** Gibt die Tageszeit an, zu der dieses Ereignis auf den Zielgeräten ausgelöst wird.
  - **Hinzufügen:** Speichert das Ereignis im Listenfeld. Sie können beim Konfigurieren einer Energierichtlinie beliebig viele Ereignisse hinzufügen.
  - **Aktualisieren:** Speichert Ihre Änderungen, nachdem Sie auf das Stiftsymbol geklickt und Änderungen an einem Ereignis vorgenommen haben.
- **Speichern:** Speichert die Richtlinie und schließt das Dialogfeld.
- **Abbrechen:** Schließt das Dialogfeld, ohne die Änderungen zu speichern.

Verwandte Themen

Schrittweise Anleitungen für die Konfiguration von HP Softwarerichtlinien-Einstellungen, die für Zielgeräte bereitgestellt werden können, finden Sie unter "Erstellen und Bereitstellen von HP Softwarerichtlinien-Einstellungen für HP Geräte" auf Seite 1015.